

Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761116487422>



SECURITY INTELLIGENCE
REVIEW COMMITTEE

Government
Publications

45

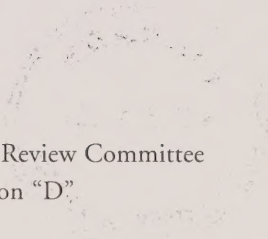
CA1
SIR
- A56

SIRC Annual Report 2005–2006

An operational review of the
Canadian Security Intelligence Service

Canada





Security Intelligence Review Committee
P.O. Box 2430, Station "D"
Ottawa ON
K1P 5W5

Tel: (613) 990-8441

Fax: (613) 990-5230

www.sirc-csars.gc.ca

Collect calls are accepted between 8:00 a.m. and 5:00 p.m. Eastern Standard Time.

© Public Works and Government Services Canada 2006

Cat. No. PS105-2006

ISBN 0-662-49440-7



SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2005–2006

An operational review of the
Canadian Security Intelligence Service





Photo: Couvrette/Ottawa

Members of SIRC (from left to right):

The Honourable Baljit S. Chadha, The Honourable Gary Filmon (Chair), The Honourable Raymond Speaker, The Honourable Aldéa Landry, The Honourable Roy Romanow

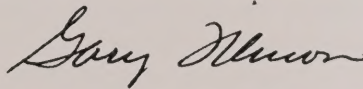
September 29, 2006

The Honourable Stockwell Day, P.C., M.P.
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6

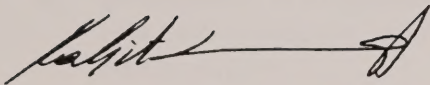
Dear Minister:

As required by Section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 2005–06, for your submission to Parliament.

Yours sincerely,



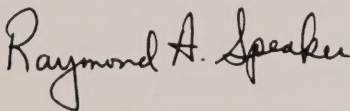
Gary Filmon, P.C., O.M.
Chair



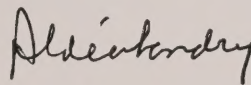
Baljit S. Chadha, P.C.



Roy Romanow, P.C., O.C., Q.C.



Raymond Speaker, P.C., O.C.



Aldéa Landry, P.C., C.M., Q.C.

Table of contents

Members' Statement	v
How this report is organized	vii
Section 1: A year in review 2005–06	1
A. Reviews of CSIS security intelligence activities	3
How SIRC carries out its review function	3
SIRC reviews in 2005–06	5
Review of a counter-terrorism investigation (# 2005–01)	5
CSIS liaison with foreign agencies: review of a security liaison post (# 2005–02)	7
Review of the Integrated Threat Assessment Centre (# 2005–03) ..	9
Review of a counter-intelligence investigation (# 2005–04)	11
Review of foreign arrangements with countries suspected of human rights violations (# 2005–06)	12
Review of CSIS's electronic-surveillance and information-gathering techniques (# 2005–07)	15
Review of activities and investigations in a CSIS region (# 2005–08)	17
B. Investigation of complaints	18
How SIRC investigates complaints	18
New procedures	22
SIRC complaint decisions in 2005–06	22
Report on the investigation into the complaint in the matter of Bhupinder Liddar (Report #1)	22
Denial of security clearance (Report #2)	23
Alleged discrimination (Report #3)	24
Alleged improper response to a complainant's illness (Report #4)	25

Section 2: CSIS accountability mechanisms	29
A. Reporting requirements	31
CSIS Director's Annual Report (2004–05)	31
Certificate of the Inspector General (2005)	32
Unlawful conduct by CSIS	32
Disclosures of information	33
B. Section 17 arrangements	34
Arrangements with domestic agencies	34
Arrangements with foreign agencies	35
C. Policy and governance framework	36
National Requirements for Security Intelligence	36
Ministerial Direction	36
Changes in CSIS operational policy	37
Governor-in-Council regulations and appointments	37
D. CSIS operational activities	37
Counter Intelligence Branch	38
Counter Proliferation Branch	39
Counter Terrorism Branch	39
Research, Analysis and Production Branch	40
Security Screening Branch	41
Foreign Liaison and Visits Branch	46
Federal Court warrants and warrant statistics	47
Integrated Threat Assessment Centre	49
Section 3: Want to know more about SIRC?	51
Committee membership	53
Staffing and organization	54
Budget and expenditures	55
Inquiries under the <i>Access to Information and Privacy Acts</i>	55
Communications	56
Modern comptrollership	57
Appendix A: SIRC reviews since 1984	59
Appendix B: Recommendations	71

Members' Statement

As the 21st century unfolds, the spectre of terrorism has become the major preoccupation of police and national security agencies. Even in those countries that have not suffered direct attacks, terrorism has sowed fear and uncertainty. The challenge for Canada is to ensure public safety without compromising the values that are the bedrock of our democratic tradition.

The Security Intelligence Review Committee (SIRC) is one of the organizations responsible for maintaining that balance. It is the only independent, external body equipped with the mandate to review the activities of the Canadian Security Intelligence Service (CSIS), by examining its operations and investigating complaints. For over two decades, SIRC has fulfilled this responsibility, always conscious of CSIS's vital role in safeguarding our society, but alert to the extraordinary powers that it is authorized to employ.

Our annual report summarizes, to the extent that national security permits, SIRC's key accomplishments in 2005–06. This year's report provides highlights of seven reviews as well as four decisions rendered in complaints cases. Among the more noteworthy reviews was an examination of CSIS's relationship with agencies in four countries suspected of human rights violations, plus our first review of the Integrated Threat Assessment Centre, a key component of Canada's National Security Policy. We also examined CSIS's electronic-surveillance and information-gathering techniques, to gain a better understanding of how rapidly evolving technologies are being used by CSIS and exploited by terrorists and foreign intelligence agencies. We made fourteen recommendations as a result of these seven reviews, which are summarized at the end of this report.

In addition to conducting reviews, SIRC is also responsible for investigating complaints against CSIS. In fulfilling this role, we provide an independent recourse mechanism for groups and individuals, with all the powers of a superior court. Over the past two decades, SIRC has issued 125 decisions related to complaints, each of which stands as a testament to our fairness and objectivity. In 2005–06, SIRC dealt with 63 complaints—a significant increase over recent years—and issued four new decisions. Among these is a Section 42 complaint concerning the denial of a security clearance to Mr. Bhupinder Liddar, where SIRC found in favour of the complainant.

Innovative procedures designed to modernize the complaints function are also highlighted in this year's report. In an effort to be more inclusive, we posted an Arabic translation of "How To Make A Complaint" on SIRC's website. In consultation with CSIS, we introduced pre-hearing conferences to resolve preliminary procedural matters and adopted the principle of continuing disclosure, so that new documents can be introduced at any time before a decision is rendered. We are proud of these innovations because they have streamlined our investigation process and over time, will help to ensure that SIRC's recourse mechanism is better understood.

Accountability is the *raison d'être* of review and oversight agencies around the world. That is why we felt it so important to contribute to the work of the O'Connor Commission, which is tasked with making recommendations on an independent, arm's-length review mechanism for the RCMP's national security activities. During the past year, our Chair discussed this subject at a public hearing of the Commission and SIRC staff held wide-ranging discussions with their Commission counterparts. Mr. Justice O'Connor's recommendations will likely focus considerable public attention on the adequacy of Canada's review mechanisms, and we will be very interested to see how the federal government responds.

A society that bends the rules confirms the worst prejudices and suspicions of its enemies, while individual rights are meaningless without real and lasting human security.

As stated previously, terrorism poses significant and continuing challenges to Canada and other western democracies. As free societies, we are compelled to use every available resource to counter this deadly threat, while at the same time upholding the principles of accountability, fairness, respect for individual rights and an absolute adherence to the rule of law.

If we can leave our readers with one message, it is this: do not assume that the demands of public safety and our democratic values are in an irreconcilable conflict with each other. In fact, they are complementary. A society that bends the rules confirms the worst prejudices and suspicions of its enemies, while individual rights are meaningless without real and lasting human security. That is why it is so important that police and national security agencies are held accountable for their actions and choices.

For twenty-two years, SIRC has strived to ensure real accountability by upholding Canadians' fundamental rights and freedoms and by insisting that CSIS act lawfully. This is our legacy and our continuing commitment to Parliament and the citizens we serve.

How this report is organized

The Security Intelligence Review Committee provides assurance to the Parliament of Canada—and through it, to Canadians—that CSIS is acting lawfully in the performance of its duties and functions. SIRC has two key functions. The first is to conduct in-depth reviews of CSIS activities to ensure that they comply with the *CSIS Act* and the various policy instruments that flow from it, and with direction from the Minister of Public Safety. The second is to receive and investigate complaints by any person about any action of the Service.

SIRC's 2005–06 annual report is organized to reflect key findings and recommendations arising from its reviews and complaints investigations. Also included is more general background material, collected to inform Committee Members and to assist readers in understanding the broader context in which CSIS's security intelligence work is carried out. The report's three sections are summarized as follows:

Section 1: A year in review 2005–06

This section summarizes seven reviews SIRC conducted during the period covered by this report. It also provides information about complaints received by SIRC.

Section 2: CSIS accountability mechanisms

Featured in this section are descriptions of the policy and governance framework within which CSIS carries out its duties and functions. This section also contains information provided by CSIS on operational activities, plans and priorities, organized according to the Service's major branches.

Section 3: Want to know more about SIRC?

This section provides details about the information gathering, outreach, liaison and administrative activities of SIRC, including its annual budget and expenditures.

Section 1

A year in review 2005–06

A year in review 2005–06

A. Reviews of CSIS security intelligence activities

HOW SIRC CARRIES OUT ITS REVIEW FUNCTION

The Security Intelligence Review Committee is the only independent, external body equipped with the legal mandate and expertise to review the activities of CSIS. SIRC was established under the *CSIS Act* (1984) to provide assurance to the Parliament of Canada and to Canadians that CSIS is complying with law, policy and Ministerial Direction in the performance of its duties and functions. In doing so, SIRC seeks to ensure that the fundamental rights and freedoms of Canadians are respected.

To fulfill its mandate, SIRC directs staff to undertake a number of reviews each year. These provide a retrospective examination and assessment of specific CSIS investigations and functions. Under the *CSIS Act*, SIRC has virtually unlimited power to review CSIS's performance. With the sole exception of Cabinet confidences, SIRC has the absolute authority to examine all information concerning CSIS's activities, no matter how highly classified that information may be.

Each review includes SIRC's findings and recommendations. Upon completion, the report is forwarded to the Director of CSIS and the Inspector General of CSIS.

SIRC is also authorized under Section 54 of the *CSIS Act* to provide special reports to the Minister of Public Safety on any matter that Committee Members identify as having special importance or that the Minister requests SIRC to undertake.

What's the difference between an oversight and a review agency?

An oversight body looks on a continual basis at what is taking place inside an intelligence service and has the mandate to evaluate current investigations or work in "real time." SIRC is a review body, so unlike an oversight agency, it can make a full assessment of CSIS's past performance without being compromised by any involvement in its day-to-day operational decisions and activities.

SIRC's research program is designed to address a broad range of subjects. In deciding what to review, SIRC considers:

- priorities and concerns identified by Parliament or in the media;
- particular activities that could intrude on individual rights and freedoms;
- the CSIS Director's classified report to the Minister;
- the need to assess regularly each of the Service's branches and regional offices;
- SIRC's statutory authorities as detailed in the *CSIS Act*;
- events with the potential to cause threats to the security of Canada;
- commitments by SIRC to re-examine specific matters;
- issues identified in the course of SIRC's complaints function; and
- new policy directions or initiatives announced by CSIS or the Government of Canada.

This approach allows SIRC to manage the inherent risk of being able to review only a small percentage of CSIS activities in any given year. Each review results in a "snapshot" of the Service's actions in relation to applicable laws, policies and Ministerial Direction. Over the past two decades, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities, and assurance that CSIS is acting lawfully.

SIRC is but one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through the existing apparatus of government, specifically the Minister of Public Safety, the Inspector General of CSIS, central agencies, as well as the Auditor General, the Information Commissioner, and the Privacy Commissioner of Canada.

SIRC REVIEWS IN 2005–06

Review of a counter-terrorism investigation

Report # 2005–01

Background

This review focused on a CSIS investigation of a terrorist organization suspected of raising funds in Canada for its activities abroad.

Methodology

SIRC examined this investigation for the period from January 1, 2004–January 31, 2005. It reviewed hard-copy and electronic documentation pertaining to the following operational activities of the Service:

- the targeting of individuals suspected of engaging in threat-related activities, as well as the targeting-approval process;
- the direction of human sources against authorized targets;
- all exchanges of information with domestic partners; and
- advice to government.

Findings

Overall, the Service's activities were in compliance with the *CSIS Act*, Ministerial Direction and operational policy during the review period. SIRC found that CSIS had reasonable grounds to suspect that the targets of the investigation posed a threat to the security of Canada and that the targeting authorities were proportionate to the seriousness of the threats. CSIS investigators collected only information that was strictly necessary to the investigation.

Further, the Service's use of human sources and its exchanges of information with domestic partners complied with the *CSIS Act* and applicable Ministerial Direction. Although there were a few administrative errors in CSIS's management of sources, they did not affect the quality of the investigation, nor did SIRC see them as serious. SIRC also found that all reports CSIS distributed to senior government officials accurately reflected information in its operational reports.

SIRC was concerned about one exchange of information involving a foreign agency and noted a problem that arose as a consequence of a domestic partner's misuse of CSIS information.

SIRC also learned that CSIS's investigation of the terrorist organization brought it into contact with a sensitive Canadian institution.

CSIS has a mandate to investigate threats to the security of Canada, no matter how sensitive the venue in which those threats arise. Nevertheless, certain Ministerial Directions and operational policies require CSIS to take particular care when there is the possibility that its investigative activities will bring it into contact with a sensitive Canadian institution, which includes the academic, media, political, religious and trade union sectors.

In accordance with Section 2 of the *CSIS Act*, when investigating activities that pose a threat to the security of Canada, CSIS is prohibited from investigating those involving lawful advocacy, protest and dissent unless they are carried on in conjunction with threat-related activities. However, there are occasions when it will investigate groups or individuals who simultaneously engage in a legitimate political activity and a threat-related activity; who engage in a threat-related activity under the guise of a legitimate political activity; or who engage in a legitimate political activity that evolves into a threat-related activity.

These policies are more stringent than those governing other aspects of CSIS operations. They require that CSIS balance the use of intrusive investigative techniques against possible damage to civil liberties or to these fundamental societal institutions. This review identified an area where, in SIRC's opinion, operational policy needs to be expanded to cover CSIS's contact with the sector in question.

SIRC therefore recommended that CSIS extend its sensitive sector policy to require senior-level approval for certain investigative techniques. It is worth noting that SIRC made a similar recommendation in last year's annual report (see SIRC study # 2004–06).

CSIS liaison with foreign agencies: review of a security liaison post

Report # 2005–02

Background

CSIS maintains a number of Security Liaison Officer (SLO) posts outside Canada. With the exception of Washington, London and Paris, the location of these posts is classified. This year, SIRC reviewed one of the busiest of these posts, which receives thousands of messages annually and has numerous exchanges with foreign security and intelligence agencies located in that country.

Methodology

SIRC's objective was to determine whether the exchanges of information with the foreign agencies at this post were within the scope of the approved liaison agreements in place. SIRC also assessed whether activities at this post complied with the *CSIS Act*, with Ministerial Direction and with the Service's operational policies and procedures.

SIRC conducted this study by reviewing documents at CSIS Headquarters, as well as through on-site visits to the post. For context, the report also considered trends identified in previous SLO studies and SIRC's ongoing reviews of CSIS's foreign arrangements.

Findings

SIRC found that the SLO post in question was managed effectively and that its operations complied with the *CSIS Act*, Ministerial Direction, as well as with CSIS operational policy and guidelines.

SLOs:

- carry out regular liaison with foreign security and intelligence agencies;
- provide security screening services in support of Canada's immigration program;
- carry out the exchange of security intelligence information with approved agencies; and
- provide advice to senior staff of the Canadian Mission or Embassy.

SIRC made five recommendations.

First, SIRC reiterated a recommendation from its Section 54 report on Maher Arar—that **CSIS Security Liaison Officers should maintain a written record when requests for information from CSIS Headquarters are transmitted verbally to foreign intelligence agencies.**

The four remaining recommendations concerned issues related to the documentation used by CSIS to manage its foreign relationships.

SIRC recommended that CSIS update the post profile.

To ensure that CSIS Headquarters and SLOs are kept apprised of information exchanged with foreign partners, operational policy requires that CSIS employees submit a written report following a contact or visit with a representative of a foreign service. Not only are these reports important for managing CSIS's foreign relationships, they also help to keep the appropriate SLOs informed of discussions with foreign agencies and of information exchanged with their foreign counterparts. During the review period, such reports were not submitted regularly to CSIS Headquarters by the post. **SIRC recommended that CSIS Headquarters remind operational branches and SLOs to submit these reports in a timely fashion.**

SIRC also recommended that CSIS produce an assessment document concerning a new relationship with a specific foreign agency, especially since CSIS Headquarters made the same request in 2003.

Finally, with respect to CSIS's documentation of a separate and relatively new foreign arrangement with a particular intelligence agency, SIRC noted a lack of any written documentation regarding possible human-rights concerns cited by organizations such as Amnesty International and Human Rights Watch. As a result, **SIRC recommended CSIS develop an operational policy for documenting its relationships with agencies that are known or reputed to have engaged in human-rights abuse.**

Review of the Integrated Threat Assessment Centre

Report # 2005–03

Background

In April 2004, the Government of Canada announced *Securing an Open Society: Canada's National Security Policy*. One outcome was the establishment of the Integrated Threat Assessment Centre (ITAC) in July 2004, to ensure that terrorist threat assessments can be quickly transmitted to those decision-makers who need this information. It officially opened in October 2004.

ITAC allows for increased involvement by municipal and provincial authorities in evaluating and countering threats to Canada's national security. Located at CSIS Headquarters, ITAC is a functional component of the Service. It is governed by the *CSIS Act*, Ministerial Direction, CSIS operational policies, and is subject to review by SIRC.

Many within the security and intelligence community have adopted the term "fusion centres" when referring to the integration of all information relevant to the security and defence of a country.

ITAC brings together analysts, security experts, enforcement and intelligence officials from the Canada Border Services Agency, the Communications Security Establishment, the Department of National Defence, Foreign Affairs Canada, Privy Council Office, the Ministry of Public Safety, Transport Canada, Ontario Provincial Police, Sûreté du Québec, RCMP and CSIS.

The ITAC Director is appointed by the National Security Advisor to the Prime Minister, in consultation with the Director of CSIS. The current ITAC Director, seconded from the RCMP, was appointed in July 2005 for a two-year term. CSIS's role with respect to other ITAC partners is one of first among equals. The Service supplies the Centre's administrative, security and support services and administers its budget.

Methodology

This review was a foundation study to be used as a basis for future SIRC reviews. SIRC examined all available documentation concerning the formation and operations of ITAC, as well as its predecessor, the Integrated National Security Assessment Centre (INSAC).

SIRC was provided with all threat assessments produced by INSAC between February 2003 and July 2004, as well as ITAC threat assessments produced between October 2004 and February 2005. Of these, SIRC reviewed a sample of INSAC and ITAC reports to assess whether drafting, review and distribution processes complied with the *CSIS Act*, Ministerial Direction and operational policy.

Findings

SIRC found that, for the most part, the Service complied with the *Act* as well as Ministerial Direction. However, SIRC also found that the Service had not yet integrated the operations of the Centre into existing operational policies or approved new ITAC-specific policies. **SIRC recommended that CSIS review its policies to determine where ITAC-specific amendments are required to address the role of this organization.**

ITAC produces assessments that warn the government about terrorist threats to Canada and to Canadian interests abroad. The Centre consults with its partners and clients in identifying specific topics, and with an advisory committee to develop its work plan. Each assessment integrates open-source and classified intelligence obtained from various domestic and foreign agencies. Classified information is extracted by ITAC staff on-site from partner agencies' respective electronic networks that hold criminal, intelligence and immigration information. SIRC found that ITAC's electronic capacity gives it unprecedented and far-reaching access to Canadian intelligence sources.

Once completed, ITAC's threat assessments are distributed to agencies and departments at the federal, provincial, territorial and municipal levels of government, as well as to Canadian law enforcement agencies. They are also provided to foreign agencies. SIRC found that most of these exchanges were conducted using approved CSIS cooperation agreements with foreign security and intelligence agencies. However, the Committee noted that CSIS was exchanging information with another foreign fusion centre without a Section 17 arrangement, as required under the *CSIS Act*. **SIRC recommended that CSIS formalize its relationship with this centre and seek an approved foreign arrangement from the Minister of Public Safety.**

ITAC also redistributes within the Canadian government the threat assessments produced by counterparts in the United States, the United Kingdom, Australia and New Zealand. These assessments accounted for almost three-quarters of all reports distributed by ITAC between October 2004 and August 2005. SIRC noted that, as of January 2005, ITAC was in the process of analyzing distribution problems and was studying its network to identify bottlenecks.

Review of a counter-intelligence investigation

Report # 2005–04

Background

SIRC examined a long-running counter-intelligence investigation, which was last reviewed in 1996. A foreign intelligence service was suspected of covert espionage and foreign interference in Canada, as defined by Sections 2(a) and 2(b) of the *CSIS Act*.

CSIS sought to identify which sectors or industries (aeronautical, telecommunications, military, scientific or technological) were being targeted by the foreign intelligence service. It also looked into suspected incidents of spying on expatriates who had relocated to Canada.

According to Section 2(a) of the *CSIS Act*, “espionage... that is against Canada or detrimental to the interests of Canada or activities directed toward or in support of such espionage” are threats to the security of Canada.

Section 2(b) defines foreign interference threats as “foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person.”

Methodology

SIRC’s review concentrated on the Service’s management of this investigation between January 2002 and December 2004, plus some material outside of the review period. This included hard-copy and electronic documentation related to targeting decisions and the management of human sources.

Findings

Overall, the counter-intelligence investigation complied with the *CSIS Act*, Ministerial Direction and operational policy during the review period.

SIRC concluded that:

- CSIS had reasonable grounds to suspect that this foreign intelligence service or its agents posed a threat to the security of Canada;
- the level and intrusiveness of the investigation were proportionate to that threat; and
- the Service only collected information strictly necessary to fulfill its mandate.

CSIS's investigation was terminated during the review period. SIRC noted that CSIS had thoroughly investigated all suspected espionage and foreign interference activities, and was satisfied that these were either unsupported by corroborative evidence or were isolated incidents. Further, the Service assured SIRC it was prepared to deal on a case-by-case basis with any future threats posed by the foreign intelligence service in question.

Based on the information available for its review, SIRC accepted the Service's evaluation that this foreign intelligence service no longer presented a threat to the security of Canada.

There were no recommendations arising from this review.

Report # 2005–05

Note:

SIRC is currently working on review # 2005–05, but it had not been finalized at the time this annual report went to print. A summary of this review will appear in SIRC's 2006–07 annual report.

Review of foreign arrangements with countries suspected of human rights violations

Report # 2005–06

Background

The *CSIS Act* authorizes CSIS to enter into arrangements with foreign intelligence agencies for purposes of exchanging information concerning threats to the security of Canada. In cases involving countries that have a questionable commitment to human rights, Ministerial Direction stipulates that arrangements will be considered only if they are required to protect the security of Canada. Once an arrangement is established, CSIS continues to monitor the foreign agency's human rights record through annual assessments.

As provided under Section 38(a)(iii) of the *CSIS Act*, SIRC reviews these arrangements and monitors the information and intelligence that is exchanged. This year, SIRC chose to review CSIS's relationships with agencies from four countries suspected of human rights violations.

Methodology

This study examined CSIS's foreign arrangements with seven foreign agencies, as well as information exchanged as a result of these arrangements.

For each foreign agency, SIRC examined:

- the rationale for establishing and—if applicable—expanding the arrangement;
- the relationship between CSIS and the agency;
- the nature of the information exchanged;
- special conditions or limitations on the collection or use of information; and
- an assessment of the intelligence disclosed to—and received from—the foreign agency.

The review covered the period January 1, 2002–December 31, 2004. Some information was also requested outside this period.

Findings

Overall, SIRC found that CSIS's exchanges of information with these agencies were within the scope of the respective foreign arrangements, and that the Service complied with the *CSIS Act*, Ministerial Direction and operational policies.

However, SIRC did note some concerns. First, it found that, even though CSIS was fully compliant in providing certain information to a foreign agency, this could have contributed to that agency's decision to detain a Canadian citizen (who was also a CSIS target) upon arrival in that foreign country.

Second, SIRC was concerned that, even though CSIS was fully compliant in conducting the exchanges in question, information the Service received and used from a foreign agency may have been obtained under duress. SIRC also noted that questions submitted by CSIS to this agency via a third party may have been used in interrogating a Canadian citizen in a manner that violated his human rights. CSIS had assessed both of these individuals as posing a threat and it obtained the necessary authority to launch investigations. However, it is outside SIRC's capacity to review whether other domestic or foreign agencies, who were also investigating these individuals, may have contributed to these individuals' detention and/or questioning.

SIRC believes that CSIS's policy framework should reflect the challenges of dealing with countries suspected of human rights violations.

Regarding information that could have been obtained through human rights violations, SIRC asked whether CSIS treated it differently than information received by other means. CSIS replied that it takes “no piece of information at face value and must find a way to independently corroborate the information before an assessment as to the reliability of the information is assigned.” CSIS further acknowledged that in most cases, it “will not know whether a piece of information originated from an abuse of human rights, [but] if suspected, the Service has to balance that against the need to secure information to protect Canadians and Canadian interests.”

CSIS noted that employees are expected to scrutinize closely the information received or exchanged with agencies in countries with questionable human rights records, and are encouraged to use due diligence when assessing the information obtained. While the Service indicated that human rights issues are taken into account during the exchange process, there is currently no specific operational policy requiring that it do so.

SIRC recognizes that for CSIS to safeguard Canada’s national security the Service must maintain relationships and exchange information with agencies around the world—some of whom have questionable human rights records. Nevertheless, SIRC believes that CSIS’s policy framework should reflect the challenges of dealing with countries suspected of human rights violations.

SIRC recommended that CSIS amend its policy governing the disclosure of information to foreign agencies, to include consideration of the human rights record of the country and possible abuses by its security or intelligence agencies.

As part of its review, SIRC also noted references to secure telephone conversations that took place between a Security Liaison Officer (SLO) stationed abroad and CSIS Headquarters. When SIRC inquired about the content of these conversations, the Service responded that there were no written records of these verbal discussions.

As a result, SIRC recommended that CSIS Headquarters should maintain a written record of secure telephone conversations with SLOs—specifically conversations that contain operational information—and include this in its reporting.

SIRC also learned that detailed discussions on the parameters and terms of arrangements are usually held between CSIS and the foreign agencies only after a foreign arrangement has been established. SIRC believes that these issues should be raised earlier in the process of establishing such arrangements.

SIRC recommended that CSIS review its procedures so that the parameters and methods of exchange—as well as the Service’s expectations—are communicated to the foreign agency prior to entering into new foreign arrangements.

Review of CSIS's electronic-surveillance and information-gathering techniques

Report # 2005–07

Background

When CSIS was created in 1984, there were fewer than ten major telephone companies operating in Canada, and it would be a decade before the Internet would become a household word. Since then, telecommunications services have grown exponentially, as have the online activities of Canadians.

Rapidly evolving technologies have resulted in dramatic changes to the types of techniques that can be used to conduct electronic surveillance. Advances in broadband and wireless communication are increasingly challenging the ability of CSIS and police to lawfully access information needed to ensure public safety. Currently Canadian telephone and Internet service providers are not required to build or maintain intercept capabilities in their networks. As a result, when a new technology is introduced, CSIS and the police often have to research and engineer unique and costly means of gaining lawful access to these networks.

The pace of technological change—and the speed with which terrorists and foreign intelligence agencies are adopting these innovations—means that Canadian law enforcement and security agencies must stay abreast of new developments. So too must SIRC, to continue to perform its review function.

Section 21(3) of the *CSIS Act* permits the Service, with the authorization of a Federal Court judge, to “intercept any communication or obtain any information, record, document or thing.” However, Canada is one of the few G-8 countries that does not have legislation outlining mandatory requirements for companies to provide interception capability. The proposed *Modernization of Investigative Techniques Act* would have addressed this deficiency.

Some groups expressed concern about the impact that this proposed legislation could have had on privacy rights in Canada. SIRC believes that these concerns could be accommodated, however, in a modernized legislative framework, bringing Canada in line with other close

The Government of Canada introduced the *Modernization of Investigative Techniques Act* in November 2005, but the bill only received its first reading before Parliament was dissolved prior to the federal election. Similar legislation has, however, been in place for several years in other countries, including the United States, the United Kingdom and Australia. More information is available at the Public Safety website (www.psepc-sppcc.gc.ca).

allies. It is worth noting that a 2006 public opinion survey suggested that 49 per cent of Canadians believe that police and intelligence agencies should have more powers to ensure security, even if it means Canadians have to give up some personal privacy safeguards.¹

Methodology

SIRC reviewed two warrant applications approved by the Federal Court in 2004, one for a counter-intelligence investigation and the other for a counter-terrorism investigation. SIRC examined hard-copy and electronic documentation pertaining to each of the warrant applications, as well as the implementation of warrant powers against authorized targets.

Findings

SIRC found that the Service complied with the *CSIS Act* and all relevant operational policies in its application for, and execution of, warrant powers in support of the counter-intelligence investigation.

Contrary to operational policy, SIRC found that CSIS continued to collect information on a counter-terrorism target for a short period of time after terminating its investigation. CSIS confirmed, however, that it did not process this information and that it subsequently deleted the information. In addition, SIRC was unclear why CSIS believed that warrant powers were necessary to investigate another counter-terrorism target.

SIRC also noted some administrative delays within CSIS in submitting documents related to the implementation of warrant powers against certain counter-terrorism targets. It also found that several other warrant implementation files did not contain all the documents required by operational policy.

SIRC agreed with CSIS that different situations may require different types of documentation and that these requirements may change over time. In the interest of accountability and efficiency, however, **SIRC recommended that CSIS review and revise the warrant policy in question so that it reflects current best practices.** Pursuant to this recommendation, the Service has undertaken to revise its policy in this regard.

¹ *Security Monitor (Wave 6)*, Ekos Public Opinion Research, (June 2006), page 16.

Review of activities and investigations in a CSIS region

Report # 2005–08

Background

SIRC frequently reviews CSIS's activities in a particular region of Canada. These regional reviews provide insights into how investigations authorized by CSIS Headquarters are implemented in the field, and help SIRC to gain a better understanding of a region's activities, priorities and challenges.

This regional review was timely as it allowed SIRC to examine the first warranted investigation of a new and emerging threat within Canada: homegrown Islamic extremism.

Methodology

With respect to the warranted investigation, SIRC assessed the Service's compliance with the *CSIS Act*, Ministerial Direction and relevant operational policy by examining CSIS's:

- acquisition and execution of warrant powers, along with special operations;
- targeting approval process and investigation of targets;
- recruitment, development and tasking of human sources;
- cooperation, liaison and exchanges of information with domestic partners; and
- internal security measures and procedures.

This review covered the period January 1, 2002 to December 31, 2004.

Findings

SIRC agrees with the Service's assessment that homegrown Islamic extremism is a serious threat to national security. CSIS's investigations identified several individuals involved in planning terrorist acts, or engaged in fundraising, recruitment and training. SIRC found that the region's description of threat-related activities in its requests for warrants accurately reflected the information held by the Service. Further, the scope of warrant powers requested and subsequently exercised by the Service were appropriate to the threat, and complied with the *CSIS Act*, all Federal Court conditions, as well as the Service's own operational policies.

Although human sources were handled effectively, SIRC observed that there was a lack of coordination regarding joint handling of a source by two regions. SIRC also found that one source was directed against targets within a sensitive institution prior to appropriate approval having been secured, although approval was soon granted thereafter.

SIRC had concerns about the use of a certain interception technique used by the Service and **recommended that CSIS obtain an updated legal opinion governing the use of this particular technique.**

A review of internal security measures, including violations and breaches, is a standard part of every regional review. SIRC found internal security issues were dealt with appropriately in the region, with the exception of a district office, where potential violations were not documented. Although SIRC was assured that other internal safeguards would have prevented any violation, **SIRC recommended that existing operational policy be strictly adhered to by all regions, regardless of location, size or staff complement.**

B. Investigation of complaints

How SIRC investigates complaints

In addition to its review function, SIRC is responsible for investigating complaints from the public about CSIS. Almost all complaint cases begin as inquiries to SIRC— either in writing, in person or by phone. SIRC staff respond promptly to such inquiries, usually instructing the prospective complainant about what the *CSIS Act* requires for their concern to become a formal complaint. Once a written complaint is received, SIRC conducts an initial review.

SIRC has all of the powers of a superior court, and has access to all information that might be in the possession of CSIS, except for Cabinet confidences.

Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated. If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee members, assisted by staff. In investigating complaints, SIRC has all of the powers of a superior court, and has access to all information that might be in the possession of CSIS, except for Cabinet confidences.

A complainant has the right to be represented by counsel and to make representations at the hearing. Pre-hearings may be conducted to establish and agree on procedures with the complainant and/or the complainant's counsel. SIRC's Senior Counsel provides legal advice on procedural and substantive matters, and will also cross-examine Service witnesses when, for national security reasons, evidence must be heard without the complainant being present.

At the completion of a hearing, SIRC prepares a report with findings, including any recommendations SIRC considers appropriate. This report is sent to both the Minister of Public Safety and the Director of CSIS. Any information with national security implications is removed from the version of the report that goes to the complainant. Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC's annual report to Parliament.

Types of complaints

Four kinds of matters may be investigated by SIRC:

- complaints lodged by persons “with respect to any act or thing done by the Service” (Section 41);
- complaints received concerning denials of security clearances to government employees or contractors (Section 42);
- referrals from the Canadian Human Rights Commission of allegations made to it; and
- Minister’s reports in regards to the *Citizenship Act*.

The types of complaints that SIRC investigates are described in the *CSIS Act* and take several forms. Under Section 41 of the *Act*, SIRC can investigate “any act or thing” done by the Service. Under Section 42, it can hear complaints about denials of security clearances to federal government employees and contractors (*see “Determining jurisdiction of a complaint under Section 41 and 42”*). Section 42 does not permit SIRC to accept jurisdiction to hear complaints concerning less intrusive background screening or reliability checks, which are generally conducted simply to determine the trustworthiness or suitability of a potential federal employee. These complaints are addressed through an organization’s designated grievance procedure.

Under the *CSIS Act*, individuals who have been denied a security clearance must be informed of this action by the Deputy Head of the organization. These individuals have the right to make a complaint to SIRC, and where appropriate, it will investigate and report its findings and any recommendations to the Minister, the Director of CSIS and the Deputy Head. SIRC also provides the complainant with a report of its findings, taking into consideration the obligation to protect classified information.

Should the Canadian Human Rights Commission receive a written notice from a Minister of the Crown about a complaint that relates to the security of Canada, the Commission may refer the matter to SIRC. Upon receipt of such a referral, SIRC carries out an investigation and reports its findings to the Commission, the respondent and the complainant. SIRC also has the authority to conduct investigations into matters referred to SIRC pursuant to the *Citizenship Act*.

Determining jurisdiction of a complaint under Section 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by “any person” with respect to “any act or thing done by the Service.” Before SIRC investigates, two conditions must be met:

1. the complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

Under Section 41(2) of the *Act*, SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act* (formerly known as the *Public Service Staff Relations Act*).

Determining jurisdiction of a complaint under Section 42

With respect to decisions by federal deputy heads to deny security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

1. any person refused federal employment because of the denial of a security clearance;
2. any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
3. anyone refused a contract to supply goods or services to the government for the same reason.

A complaint under Section 42 of the *Act* must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC's jurisdiction or investigated and resolved without a hearing (i.e., administrative review).

Table 1
Resolution of complaints*

	2003–04	2004–05	2005–06
Carried over	17	16	18
New	30	30	45
Total	47	46	63
Closed	31	28	39
Carried forward to subsequent year	16	18	24
Reports issued	1	3	4

** This reflects all complaints received by SIRC. Not all complaints resulted in an investigation. Some were redirected to another government institution, or were determined to be outside SIRC's jurisdiction. Others were withdrawn by the complainants.*

New procedures

During 2005–06, SIRC developed in consultation with CSIS new practices to streamline the complaints investigation process and ensure procedural fairness.

First, revisions were made to the way in which documents are disclosed to SIRC by the Service. It is important to note that SIRC's access to information in this area is limited only by Subsection 39(3) of the *CSIS Act*, which states that CSIS may withhold Cabinet confidences from SIRC. New procedures have been adopted based on the principle of continuing disclosure, as provided for in Subsection 226(1) of the *Federal Court Rules*, as well as in Subsection 6(5) of the *Canadian Human Rights Tribunal's Rules*. It allows SIRC to be notified by CSIS in a timely manner when the Service becomes aware of documents relating to a complaint that have not previously been made available to SIRC.

Another innovation is the “pre-hearing conference.” Introduced in January 2006, this conference is conducted by a presiding Member of SIRC with all parties in attendance to resolve preliminary procedural matters (e.g., allegations to be investigated, the identity and number of witnesses to be called). Provided that no issues of national security are raised, the conference can be conducted by telephone and a transcript is later provided to the parties.

As of March 31, 2006, four pre-hearing conferences had been held by SIRC.

SIRC complaint decisions in 2005–06

The following are summaries of the decisions rendered by SIRC during the period under review, in response to complaints filed with SIRC.

Report on the investigation into the complaint in the matter of Bhupinder Liddar

REPORT #1

A complaint was filed with SIRC under Section 42 of the *CSIS Act* after the complainant, Mr. Bhupinder Liddar, was denied a security clearance, based on a recommendation (referred to as a “denial brief”) by CSIS.

After reviewing the complaint, SIRC found there was no reasonable basis for that recommendation, and that it was inaccurate and misleading for several reasons.

First, SIRC concluded that the denial brief contained an unfair and prejudicially inaccurate account of the information that the Service had in its possession when it began the security clearance investigation. Next, SIRC concluded that the brief was based on a field investigation conducted by an inexperienced CSIS investigator, who arrived at unfounded conclusions.

SIRC found that there was no reliable evidence to support a conclusion that the complainant might engage in activities that would constitute a threat to the security of Canada, or that the complainant might disclose classified information in an unauthorized way.

SIRC recommended that:

- **The Deputy Head of the relevant federal department/agency grant the complainant the requested security clearance; and**
- **CSIS institute procedures to ensure that accurate notes are taken, or that a recording is made, of security screening interviews. These should be kept for five years after an interview, or for even longer periods should an interviewee challenge the outcome of a security screening investigation.**

In response to this latter recommendation, CSIS informed SIRC in December 2005 that it had revised its practices concerning note-taking and consensual recording of interviews. Investigators are now required to make an offer to record an interview of a subject when conducted for government security screening. The Service will continue its requirement to prepare an accurate, complete report of the proceedings, regardless of whether the subject consents to the interview being recorded.

Denial of security clearance

REPORT #2

SIRC reported a second decision that was also pursuant to Section 42 of the *CSIS Act* concerning the denial of a security clearance.

SIRC found that the decision to deny the security clearance was made on incomplete and at times incorrect information. Some corroborated information that was favourable to the complainant was not included in the denial brief. Moreover, SIRC found that concerns identified by the employing department about the complainant's loyalty and reliability were not supported by the evidence presented during the complaints hearing.

SIRC also found that there was a lack of procedural fairness in this case by the employing department, since the complainant was not able to respond to the allegations prior to the decision to deny the security clearance. The complainant was not made aware by the employing department of the reasons for the denial, including the security concerns identified by CSIS.

SIRC recommended that:

- the complainant be granted the requested security clearance;
- CSIS should verify or corroborate security clearance information provided by an applicant or by sources when it can be done easily;
- the employing department/agency should clarify its procedures so that an individual in these circumstances is provided with information concerning any adverse findings by CSIS. This should be done in a manner that respects national security, but provides the individual with an opportunity to know the reasons for a denial of security clearance;
- both CSIS and the employing department/agency give consideration to recent remarks by the Privacy Commissioner—that as law enforcement and national security agencies collect more information from more sources, there is a greater chance that information of questionable accuracy could influence decisions or be taken out of context²;
- the Minister responsible for the employing department/agency write to and inform the complainant's former Member of Parliament that—contrary to earlier information—there was no evidence that the complainant's character or past association would affect the individual's suitability to be granted a security clearance at any level; and
- the employing department/agency take measures to ensure the quality and the accuracy of information that is transcribed from hand-written personal history forms.

Alleged discrimination

REPORT #3

SIRC reported a decision concerning a complaint that was referred to SIRC by the Canadian Human Rights Commission under Section 45 of the *Canadian Human Rights Act* (CHRA).

² See Office of the Privacy Commissioner, *Annual Report to Parliament (2004): Report on the Personal Information Protection and Electronic Documents Act*, (page 15).

The complainant—a former CSIS employee—was suffering from an illness that meets the definition of disability as provided under the *CHRA*. It was alleged that the Service had failed to accommodate the complainant's disability, and instead allegedly took advantage of that disability to obtain statements and cause termination of employment. It was further alleged that CSIS had refused the complainant's request for an extension of the 25-day limit for appealing or grieving a dismissal.

SIRC found that the complainant, when working for CSIS, was suffering from a disability consistent with Section 7 of the *CHRA*. SIRC also concluded that there was evidence the Service either knew or ought to have known that the complainant was suffering from a disability.

SIRC determined that the complainant was treated in an adverse manner by CSIS because CSIS relied on statements previously made by the complainant as the grounds for the termination of employment. Therefore, SIRC agreed that the complainant presented a legitimate case of discrimination on a ground prohibited by the *CHRA*. The Committee maintained that CSIS should have accommodated the complainant by requesting a health review, and should have provided the complainant with an opportunity to respond to allegations prior to termination of employment.

SIRC recommended that:

- CSIS's human resources policies on Health Review be amended to require supervisors and other staff to inform their managers or the manager of an employee in question when they have reason to believe that an employee is in need of medical assistance;
- the Service allow the complainant to submit a grievance; and
- should the Canadian Human Rights Commission investigate the complainant's allegations, the CHRC should not publicly release any information identified in SIRC's report that is subject to national security considerations.

Alleged improper response to a complainant's illness

REPORT #4

SIRC reported a decision concerning a complaint pursuant to Section 41 of the *CSIS Act*, which states that any person may make a complaint about "any act or thing done by the Service."

The complainant—a former CSIS employee—alleged that CSIS had:

- pressured the complainant to remain in the workplace and to confess to actions that this individual did not commit;
- breached the Employees Assistance Program’s (EAP) code of confidentiality; and
- failed to assist the complainant when in need of medical treatment.

SIRC found that the cumulative effect of the stress and exhaustion, combined with the uncertainty of the outcome of the disciplinary process, induced the complainant to remain in the workplace, and to make incriminating statements in circumstances that rendered the statements unreliable. SIRC further maintained that CSIS failed to both assess the reliability of the complainant’s confession and provide the complainant with an opportunity to respond to a new alleged infraction prior to termination of employment.

SIRC found that a reasonable person would interpret the actions of CSIS’s Chief of Health Services—who was responsible for the EAP—as “counselling” with respect to the complainant. As a result, SIRC found that the code of confidentiality was breached when the Chief of Health Services brought an investigator to take a statement from the complainant.

SIRC recommended that the Service:

- **add a note to the complainant’s personnel file, advising that certain statements by the complainant were obtained under circumstances such that the remarks should be considered unreliable;**
- **ensure that it follows the Breach of Conduct and Discipline Policy prior to discipline being imposed on an employee;**
- **create a policy to require that all pertinent information having an impact on the reliability of statements (e.g., competency of the person to make a free and voluntary statement) be included in all internal security investigation files;**
- **remind its employees that all their written records may be subject to the *Access to Information Act*, the *Privacy Act*, as well as to operational policy, and that these should only be disposed of in accordance with the Service’s disposal-of-records policies;**
- **create a policy to require that a written record be kept of an assessment by senior management regarding the reliability and relevance of oral and written statements before deciding how to conclude an internal security investigation;**

- post a notice at the offices of Health Services and on any website pertaining to the Service's EAP that any communication other than with a counsellor, as defined by the EAP policy, will not be subject to any code of confidentiality. Staff working for the EAP must declare to participants seeking assistance under the EAP that only communications with a counsellor will be subject to the code of confidentiality;
- amend its EAP policy to require that reasonable steps be taken to ensure any required consent provided by an employee is given freely and voluntarily, and that a record of those steps should be kept on the employee's file; and
- amend CSIS's human resources policies to require that supervisors and other staff inform their managers or the manager of an employee in question when they have reason to believe that an employee is in need of medical assistance.

Section 2

CSIS accountability mechanisms

CSIS accountability mechanisms

A. Reporting requirements

CSIS DIRECTOR'S ANNUAL REPORT (2004–05)

Every year, the Director of CSIS must submit a Top Secret report to the Minister of Public Safety, describing in detail the Service's priorities and operational activities. The *CSIS Act* requires that the Inspector General of CSIS examine this report and submit a certificate to the Minister, attesting to the extent to which he or she is satisfied with its contents. Finally, the Minister sends a copy of both documents to SIRC for its review, as required by Section 38(a) of the *CSIS Act*.

The 2004–05 Director's report stated that in supporting the Service's highest priority—public safety—CSIS is working to prevent a terrorist attack from either occurring or originating in Canada. The Director noted that this is having an impact on the agency's resources, and discussed the strategies being used to combat this challenge.

Attention was also drawn to a new dimension of the threat posed by Islamic extremism. While the threat from al-Qaida remains strongest overseas, a terrorist attack on Canadian soil is now considered probable. For the first time, CSIS also warned about the relatively new threat posed by homegrown converts.

The Director's report also noted that the Service continues to investigate attempts by foreign countries to conduct espionage and interfere with expatriate communities in Canada.

The report highlighted efforts by CSIS to strengthen its cooperation with domestic partners. The Service also reported having excellent relations with its key foreign partners, and that it had assisted foreign intelligence services in newly democratized states by providing training on the principles and techniques of intelligence collection.

The report included details about the Service's human sources and security screening programs, as well as a description of its compliance with Ministerial Direction and National Requirements from the Minister of Public Safety.

Readers should note that CSIS posts public, unclassified reports on its website (www.csis-scrs.gc.ca).

CERTIFICATE OF THE INSPECTOR GENERAL (2005)

The position of Inspector General (IG) was established in 1984 under the *CSIS Act*. The IG functions as the “eyes and ears” of the Minister of Public Safety, reviewing the Service’s operations and providing assurance that CSIS is complying with the *CSIS Act*, Ministerial Direction and operational policy.

Every year, the IG submits a certificate to the Minister stating the extent to which he or she is satisfied with the CSIS Director’s Annual Report. The certificate informs the Minister of any instances of CSIS failing to comply with either the *Act* or Ministerial Direction, or an unreasonable or unnecessary exercise of powers.

In the latest certificate, the IG noted that the Director of CSIS had reported three incidents of non-compliance with operational policy for 2004–05. The IG looked into these incidents and found that appropriate action had been taken in each case. The IG also identified two additional cases of non-compliance. However, she indicated that the only corrective action required was “a greater degree of diligence in respecting the reporting requirements.”

The IG also expressed concern about several inaccuracies she identified in the Director’s report. Two concerned statistical errors but others were, in her view, more substantive. According to the certificate, the Service has acknowledged the inaccuracies and has advised the IG that corrective steps would be taken.

The IG concluded that there had been substantial improvements in the response time of the Service in assisting her office staff with their work. “The concerns raised above,” she added, “are not intended in any way to detract from the devotion or dedication of the Service or its employees to serve Canada and to counter threats to the security of the state.”

For more information, please refer to the Inspector General’s home page on the Public Safety website (www.psepc-sppcc.gc.ca).

UNLAWFUL CONDUCT BY CSIS

Under Section 20(2) of the *CSIS Act*, the Director of CSIS must submit a report to the Minister when, in the Director’s opinion, a CSIS employee may have acted unlawfully in performing his or her duties and functions. The Minister, in turn, must send the report with his or her comments to the Attorney General of Canada and to SIRC.

In 2005–06, there were no activities requiring such a report.

DISCLOSURES OF INFORMATION

Section 19 of the *CSIS Act* prohibits information obtained by the Service in the course of its investigation from being disclosed except in specific circumstances. Of note, Section 19(2)(d) gives the Minister of Public Safety the power to override any invasion-of-privacy concerns, authorizing the Service to disclose information deemed to be in the national or public interest. When such information is released, the Director of CSIS must submit a report to SIRC. In the past, there have been only two disclosures under this section of the *Act*. In 2005–06, CSIS reported to SIRC that there were no such disclosures of information.

The Service can also disclose information in written or verbal form to any law enforcement body or federal government entity, such as the Department of National Defence and Foreign Affairs Canada. When CSIS permits the use of its information by the RCMP for use in judicial proceedings, it must do so in writing.

A disclosure letter from CSIS permits the RCMP to use the Service's information to pursue a criminal investigation. Should the RCMP wish to use this information in a court of law, they must obtain an advisory letter from the Service granting them permission to do so.

The following table summarizes the Service's Section 19 disclosures by branch.

Table 2
CSIS disclosures of information under Section 19 of the *CSIS Act*

Branch	Law enforcement (a)	Foreign Affairs Canada (b)	Department of National Defence (c)	Public interest (d)
Counter Terrorism	293	0	4	0
Counter Intelligence	19	0	0	0
Counter Proliferation	23	1,340	2,353	0
Totals	335	1,340	2,357	0

(a) Disclosed under Section 19(2)(a)

(b) Disclosed under Section 19(2)(b)

(c) Disclosed under Section 19(2)(c)

(d) Disclosed under Section 19(2)(d)

Conditions for disclosure of information by CSIS

Under Section 19(2) of the *CSIS Act*, there are four situations in which the Service may disclose information obtained in the performance of its duties and functions. These are defined as follows:

- (a) information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law may be disclosed to a law enforcement agency having jurisdiction over the matter, the Minister of Public Safety or the Attorney General of the province in question;
- (b) information related to the conduct of Canada's external relations may be disclosed to the Minister of Foreign Affairs;
- (c) information related to the defence of Canada may be disclosed to the Minister of National Defence; and
- (d) information that, in the opinion of the Minister, is essential to the public interest may be disclosed to any minister of the Crown or employee of the Public Service of Canada.

B. Section 17 arrangements

ARRANGEMENTS WITH DOMESTIC AGENCIES

In carrying out its duties and functions, CSIS often collaborates with federal departments and agencies, provincial governments and law enforcement agencies. Since 9/11, more groups have become involved in national security, including police and non-governmental partners (especially concerning critical infrastructure). This creates a challenge for the Service, as it must cultivate and maintain healthy relationships with both new and existing partners to ensure that information is exchanged efficiently and that joint operations are conducted effectively.

From sharing information to conducting joint operations, domestic arrangements can take many forms. As of March 31, 2006, CSIS had 29 Memoranda of Understanding in place with domestic partners so that information could be exchanged. Of these, 17 were with federal departments or agencies, and 10 were with provincial and municipal entities (e.g., governments, agencies, police). Also of note, the arrangement with the National Security Advisor, established in 2004–05, was renewed for one more year.

Under Section 17(1) of the *CSIS Act*, the Service may, with the approval of the Minister of Public Safety, enter into an arrangement or otherwise cooperate with domestic agencies for the purpose of performing its duties and functions. Section 38(a)(iii) of the same Act authorizes SIRC to review all domestic arrangements.

ARRANGEMENTS WITH FOREIGN AGENCIES

Section 17(1) of the *CSIS Act* states that the Service can enter into arrangements with foreign agencies to exchange information concerning threats to the security of Canada. New foreign arrangements require the approval of the Minister of Public Safety, in consultation with the Minister of Foreign Affairs. Even without such an arrangement, CSIS can still accept unsolicited information from an agency or organization of a foreign country.

The Service can also expand the scope of existing active arrangements, defining the subject matter and the extent of authorized exchanges. In the case of enhanced arrangements, the Director of CSIS is granted more discretion and has the authority to approve the expansion of activities without obtaining Ministerial approval, but subject to any Ministerial caveats or instructions that may have been imposed when the initial arrangement received approval.

SIRC reviews all new, enhanced or renewed foreign arrangements, as provided under Section 38(a)(iii) of the *CSIS Act*. To do so, it examines whether:

- CSIS's foreign arrangements were in compliance with the conditions set out in the *CSIS Act*, Ministerial Direction and operational policy;
- approvals from the Minister of Public Safety and the Director of CSIS were in place when the Service began exchanging information;
- the human rights record of the foreign agency's host country—including open-source reporting from human rights agencies—was considered; and
- the most recent agency assessment met CSIS guidelines.

In 2005–06, SIRC chose to review thirteen foreign arrangements with agencies in nine countries.

SIRC found that all foreign arrangements were in accordance with the *CSIS Act*, Ministerial Direction and operational policy.

SIRC also found that the Service had informed itself of the human rights situation in all the countries and agencies in question. Moreover, the Service had proceeded cautiously with exchanges of information involving countries with questionable human rights records, although SIRC will continue to monitor one particular arrangement.

Although two assessments were not submitted on an annual basis as required, SIRC noted an improvement concerning the annual submission of agency assessments and that, overall, these met the Service's guidelines.

C. Policy and governance framework

NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE

Subsection 6(2) of the *CSIS Act* states that the Minister of Public Safety may issue written directions to the Director of CSIS. The document, entitled "National Requirements for Security Intelligence," outlines where the Service should focus its investigative efforts, and provides general direction to CSIS in its collection, analysis and advisory responsibilities. It is based on a Memorandum to Cabinet, prepared annually by CSIS for the Minister of Public Safety to present to his or her Cabinet colleagues.

In 2005–06, a Memorandum was reviewed and approved by Cabinet, but no National Requirements were issued. The Service informed SIRC that, in the absence of specific Ministerial Direction, it relied on the priorities approved by Cabinet, which would normally have served as the basis for the annual National Requirements.

MINISTERIAL DIRECTION

Under Subsection 6(2) of the *CSIS Act*, the Minister of Public Safety may issue directions governing CSIS's activities and investigations.

No new directions were issued in the year under review.

This outcome is consistent with what SIRC had predicted in its 2000–01 annual report.³ At that time, it foresaw that Ministerial Direction would likely not be

³ *SIRC Annual Report 2000–01*, page 8.

updated regularly in the future. SIRC expected that increased emphasis on the Service's own operational policies would serve as the source for special instructions and guidelines for implementation.

CHANGES IN CSIS OPERATIONAL POLICY

CSIS operational policy embodies the rules which govern the range of activities that CSIS undertakes in doing its work. Operational policy is updated regularly in accordance with legislative and other changes. These updates are reviewed by SIRC to ensure that they conform to the *CSIS Act*, Ministerial Direction and existing operational policies.

In 2005–06, CSIS was preparing for a significant reorganization of its operations, implemented in May 2006. According to the Service, an evolving threat environment required that CSIS make these changes to increase operational capability, consolidate and enhance analysis functions and enhance corporate support.⁴

CSIS revised almost 50 policies in 2005–06, of which 40 were changes reflecting the government department name change from Solicitor General to Public Safety and Emergency Preparedness Canada. Other significant influences on policy included the Service's role in assisting Canadian military operations (for which CSIS is developing a new policy), as well as the expansion of intelligence collection by CSIS overseas.

GOVERNOR-IN-COUNCIL REGULATIONS AND APPOINTMENTS

Section 8(4) of the *CSIS Act* states that the Governor-in-Council may issue regulations to the Service concerning the powers and duties of the Director of CSIS, as well as the conduct and discipline of Service employees.

The Governor-in-Council did not issue any regulations in 2005–06.

D. CSIS operational activities

The following section describes CSIS operational activities, and provides an overview of the priorities and achievements of each operational branch during 2005–06. This information provides a useful background that helps SIRC carry out its own work. It should be noted that many of the organizational units discussed below have changed as a result of the May 2006 reorganization.

⁴ CSIS press release, May 1, 2006.

COUNTER INTELLIGENCE BRANCH

The Counter Intelligence Branch focuses its operations on the hostile activities of foreign intelligence services known to be operating within Canada. The branch investigates threats to national security, including espionage and foreign-influenced activities (e.g., attempts to monitor, influence or coerce émigré communities in Canada). The branch is also responsible for investigating threats to Canadian economic security, specifically economic espionage, the clandestine acquisition of technologies and transnational criminal activity. For an example of a SIRC study in this area, see *Review of a counter-intelligence investigation (#2005–04)* in this annual report.

In 2005–06, the Service reported to SIRC that espionage activities in Canada are becoming steadily more complex and sophisticated. This is particularly true of cyber-based and other electronically-based attacks on Canadian targets. The branch reported that several successful operations were undertaken against the espionage activities of a number of foreign states.

CSIS also noted that this branch had received an increasing number of requests from other Canadian government departments to contribute its assessment and analysis on a range of issues. For example, the branch examined over 80,000 visa applications during the period under review, and successfully detected a number of known or suspected intelligence officers seeking entrance into Canada.

Table 3
Authorized targets (2005–06)

Branch	Individuals	Organizations	Issues/events	Totals
Counter Intelligence	152	36	4	192
Counter Proliferation	55	6	6	67
Counter Terrorism	274	31	30	335
Totals	481	73	40	594

COUNTER PROLIFERATION BRANCH

The Counter Proliferation Branch investigates activities related to the proliferation of weapons of mass destruction (WMD) through the development and procurement programs of foreign states of concern or terrorist organizations. The branch keeps a close watch on rogue states or groups who sponsor or commit acts of terrorism, as well as the activities of foreign intelligence services. The branch also examines the threat of chemical, biological, radiological and nuclear terrorism.

The branch reported a number of successes in its investigations, allowing the Service to play an important role in sharing intelligence with its foreign partners. It also expanded its intelligence collection activities on state-sponsored terrorism and participated in Canadian government efforts to identify covert attempts to transfer funds to international terrorist organizations.

The Counter Proliferation Branch also has units that assist other CSIS operations. These include the Threat Assessment Unit (TAU), which produces threat assessment reports on a wide range of topics, and the Immigration Assessment Unit, which liaises with the Canada Border Services Agency. TAU's assessments serve as an early warning mechanism to the government about threats to Canada and to Canadian interests abroad. In 2005–06, it produced 360 threat assessments—compared to 450 in the previous year.

COUNTER TERRORISM BRANCH

The role of the Counter Terrorism Branch is to advise the Government of Canada on threats of serious violence that could affect the safety and security of Canadians and Canada's allies.

For the fifth year in a row, Islamic extremism—particularly al-Qaida-inspired or related—remains the main concern of this branch. Moreover, the Service believes that the threat posed by these terrorist groups has increased in 2005–06. A priority of the branch is the interdiction and removal of such radicals from Canada.

The Service initiated several new investigations of alleged foreign extremists or terrorist groups that may have infiltrated into Canada. The Service also identified several previously unknown domestic extremists involved in threat-related activities. In cooperation with other domestic agencies, the branch prevented a suspected foreign extremist from entering Canada, and disrupted a Canadian-based terrorist cell.

Many of the Counter Terrorism Branch's operations are conducted in cooperation with the RCMP. The Service advises the government on threats to Canada's national security and the RCMP investigates criminal activity that poses a similar threat. Under the *Anti-Terrorism Act* (2001), the role of the RCMP in combating international terrorism was enhanced, resulting in closer ties with CSIS in matters of national security. This has resulted in successful, collaborative intelligence gathering and technical operations.

CSIS reported to SIRC that while there remains some duplication of investigations, efforts are being made within each organization to address this matter. Also, as noted in previous annual reports, CSIS continues to participate in four of the RCMP's Integrated National Security Enforcement Teams (INSETs), located in several regions across Canada. Now in its fifth year of operation, this program is projected to expand to a fifth region in 2006.

The participating CSIS regions report positive working relationships with the teams. Close cooperation and regular communication have limited potential overlap between the mandates of both organizations.

RESEARCH, ANALYSIS AND PRODUCTION BRANCH

The Research, Analysis and Production Branch produces security intelligence assessments to support the Service's operations and the Canadian government's decision-making in relation to threats to national security. It develops strategic and operational analyses of current threats and emerging issues. The *Intelligence Briefs*, *CSIS Reports* and *CSIS Studies* are the key documents prepared by this branch. CSIS produced 41 of these reports in 2005–06 and distributed them throughout the security intelligence community and to other clients.

For more information on the Terrorist Entity list, see the Public Safety website at www.psepc-sppcc.gc.ca. Readers should also refer to SIRC's study # 2004–03, summarized in SIRC's Annual Report for 2004–05.

As SIRC reported in its 2004–05 annual report, CSIS has a role in the Terrorist Entity Listing process, including developing Security Intelligence Reports (SIRs) that describe the grounds for listing an entity. These reports help the Minister of Public Safety decide whether to recommend to the Governor-in-Council to add a particular entity to the Terrorist Entity list.

In 2005–06, the branch produced nine SIRs. It also began its second two-year review of existing SIRs in the same period, to determine whether it is reasonable to maintain or to de-list an entity.

Finally, the branch supports CSIS's consultations with Foreign Affairs Canada on listing the names of persons or groups under Schedule 1 of the *United Nations Suppression of Terrorism Regulations* (UNSTR).

SECURITY SCREENING BRANCH

One of the largest branches of CSIS, Security Screening has two program streams, government screening and immigration screening.

Government screening—CSIS performs security clearance investigations for all government employees⁵ whose duties require access to classified assets or information. In each investigation, the Service provides requesting departments or agencies with a security assessment, which is an appraisal of an individual's reliability as it relates to loyalty to Canada. The largest clients of this service are Public Works and Government Services Canada (PWGSC) and the Department of National Defence (DND)—accounting for over 25 percent and 20 percent respectively of all requests in 2005–06.

As indicated in Table 4 below, CSIS received 42,100 requests for new or updated security clearances and provided 37,800 security assessments in 2005–06. Although the volume of requests increased by about 15 percent from the previous fiscal year, the number of security assessments issued by CSIS remained roughly the same, indicating that not all requests could be completed within the period under review.

Table 4
Government screening*

	2003–04	2004–05	2005–06
Requests from DND	9,900	9,100	9,200
Requests from other departments or agencies	27,600	27,400	32,900
Total	37,500	36, 500	42,100
Assessments issued to DND	10,100	9,000	8,900
Assessments issued to other departments or agencies	27,600	27,600	28,900
Total	37,700	36, 600	37,800

* Figures have been rounded to the nearest 100.

⁵ Although CSIS will provide security assessments to the RCMP based on information contained in its records, it does not conduct such investigations on behalf of Canada's national police force. The RCMP conducts these investigations on its own behalf.

To track its efficiency in responding to security screening requests, CSIS calculates its turnaround times using a median number of days.⁶ As indicated in Table 5, the median turnaround times generally decreased in 2005–06 from the previous fiscal year. There was a significant decrease in the time taken to prepare security assessments for DND at all levels.

Table 5
Median turnaround (in days)

		2003–04	2004–05	2005–06
DND	Level I (Confidential)	20	49	24
	Level II (Secret)	18	63	19
	Level III (Top Secret)	96	70	39
Non-DND	Level I (Confidential)	7	12	15
	Level II (Secret)	11	14	13
	Level III (Top Secret)	82	69	60

The Service does not issue denials of security clearance. Rather, it advises the requesting department or agency of information that would affect CSIS’s ability to recommend clearance. On rare occasions, CSIS will recommend to a requesting agency that a clearance be denied. However, it is the responsibility of the requesting agency to accept or reject this recommendation. In 2005–06, the Service issued 19 information briefs reporting information of an adverse nature, and issued one denial brief.

CSIS also provides site-access screening. Unlike a government security clearance, a site-access clearance only gives an individual access to certain secure areas within installations or provides accreditation for a special event. In 2005–06, CSIS received over 60,000 requests for this type of screening, and provided four information briefs to requesting agencies.

⁶ CSIS reports its turnaround statistics using median numbers rather than averages because this mitigates the impact of unusually short or lengthy processing times, and better represents the typical amount of time to process an assessment.

Table 6
Site-access screening programs*

	2003–04	2004–05	2005–06
Parliamentary precinct	1,400	1,100	1,000
Airport restricted-access area	28,800	31,100	37,600
Nuclear facilities	5,700	6,800	10,600
Free and Secure Trade (FAST)	N/A	21,500**	3,100
Special events accreditation	0	1,800	5,600
Other government departments	1,400	2,300	2,400
Total	37,300	64,600	60,300

* Figures have been rounded to the nearest 100.

** Refers to a one-time request to review previously granted passes, due to elevated security concerns related to the U.S. presidential elections.

CSIS advice on security screening can take one of five forms:

1. **Notices of assessment** are issued in those government and immigration screening cases when CSIS finds no adverse information on an applicant.
2. **Incidental letters** are issued to Citizenship and Immigration Canada (CIC) and to the Canada Border Services Agency (CBSA) when the Service has information about an applicant who is or has been involved in non-security related activities described under the *Immigration and Refugee Protection Act* (IRPA).
3. **Information briefs** are issued in government screening cases when CSIS has information that could have an impact on the requesting agency's decision to grant an applicant a security clearance or site access. It is also provided in immigration screening cases when the Service has information that an applicant is or was involved in activities that do not necessarily warrant inadmissibility for entry into Canada.
4. **Inadmissibility briefs** are issued to CIC/CBSA when an applicant is deemed to be inadmissible to Canada under the security provisions of the IRPA.
5. **Denial briefs** are issued when the Service recommends to a requesting agency that a security clearance or site access be denied to an individual.

Immigration screening—CSIS's Security Screening Branch also conducts investigations and provides advice to Citizenship and Immigration Canada as well as the Canada Border Services Agency to support the processing of refugee claims or applications for immigration or citizenship. The Service's authority in this regard is provided under Sections 14 and 15 of the *CSIS Act*.

In 2005–06, the branch received approximately 92,000 requests under various immigration screening programs (see Table 7)—slightly fewer than in previous years. There was a significant drop—almost 20 percent—in the number of refugee determination screening requests, compared to the previous year. Meanwhile, the number of citizenship requests almost doubled. Also of note, there was an increase—about 13 percent—in the number of immigration screening requests.

Table 7
Types of immigration screening requests

	Requests*			Briefs		
	2003–04	2004–05	2005–06	2003–04	2004–05	2005–06
Within and outside Canada	57,300	56,100	63,200	106	88	133
Front End Screening**	22,700	22,900	17,100	92	184	89
Refugee determination***	16,500	14,200	11,700	122	110	127
Subtotal	96,500	93,200	92,000	320	382	349
Citizenship applications	203,400	161,200	308,000	150	124	120
Total	299,900	254,400	400,000	470	506	469

* Figures have been rounded to the nearest 100.

** Represents those individuals who arrive at the Canadian border claiming refugee status.

*** Represents those refugees (as defined by IRPA) who apply from within Canada for permanent resident status.

The above table shows that CSIS finds no adverse information in the vast majority of its screening investigations of refugee claimants or immigration/citizenship candidates—one in every 250 immigrant applications or refugee claims screened, and one in every 2,500 citizenship applications screened. In 2005–06, of the total briefs regarding immigration screening (349), CSIS issued 232 information briefs and 117 inadmissibility briefs. There were also 12 incidental letters.

SIRC noted that generally the Service's turnaround times for the provision of information or inadmissibility briefs are quite lengthy. For information briefs related to immigration cases, it takes between 12 to 18 months to complete, depending on where the application was filed. In refugee cases, the median turnaround time was ten months for files subject to the Front End Screening program. For inadmissibility briefs, SIRC noted similar median times. For immigration files, the turnaround times ranged from a year to 18 months, while refugee files ranged from eight to 11 months.

Table 8 provides a three-year highlight of the Service's median turnaround time in providing notices of assessment.

Table 8
Median turnaround time (in days) for notices of assessment

	2003–04	2004–05	2005–06
Citizenship	1	1	1
Immigration requests from within Canada	46	44	70
Immigration requests from overseas	5	7	16
Immigration requests from the U.S.	152	150	62
Refugee determination	53	56	96
Front End Screening program	32	27	23
Visa vetting	12	13	11

Other screening activities—In 2005–06, the Security Screening Branch vetted over 36,000 visa applications of foreign nationals. It also started participating in the Free and Secure Trade (FAST) program and conducted over 3,000 security assessments of truck drivers who applied for a FAST border pass under this program. Consult the Canada Border Services Agency website at www.cbsa-asfc.gc.ca/import/fast/menu-e.html for more information on this program.

Other programs—The Front End Screening (FES) and the Electronic Data Exchange (EDE) programs were introduced in 2001 to facilitate Canada's immigration and refugee screening processes. The FES program checks all refugee applications against CSIS records to identify potential security risks as early as possible in the refugee determination process. Further information on the FES program can be found in SIRC study # 2003–01, which was summarized in SIRC's 2003–04 annual report.

The EDE is an electronic network for filing screening applications that serve to accelerate processing times. Over 50 government clients use this service, such that almost all screening requests for refugee claimants or immigration/citizenship candidates are filed electronically. As in previous years, CSIS reported to SIRC that it is continuing to expand EDE access to additional clients, including six new government clients and two new immigration posts in the fiscal year.

FOREIGN LIAISON AND VISITS BRANCH

The Foreign Liaison and Visits (FLV) Branch manages the Service's liaison with foreign agencies and coordinates visits to CSIS Headquarters and CSIS regional offices by foreign representatives. FLV is also responsible for coordinating all Section 17(1) arrangements with foreign security intelligence or law enforcement agencies, as well as the operation of security liaison posts abroad.

At the end of the 2005–06 fiscal year, CSIS had a total of 265 foreign arrangements with 144 countries. During that period, CSIS received Ministerial approval to establish six new arrangements, modify or enhance four others, and to suspend three arrangements.

Of the 265 foreign arrangements, 217 were active, 39 were dormant (i.e., no liaison contact for a period of at least one year), and nine were suspended or restricted (including the three mentioned in the previous paragraph). Any foreign arrangement classified as “dormant” or “restricted” remains as such until an update assessment of the relationship is completed.

The FLV Branch is also responsible for security liaison posts. The Service relies on these posts to liaise with foreign security and intelligence agencies. Security liaison officers are also called upon to assess the effectiveness of individual Section 17 foreign arrangements and submit annual assessments on each foreign agency in terms of their reliability as a partner, and their human rights record. For more information, see *CSIS liaison with foreign agencies: review of a security liaison post (# 2005–02)* in this annual report.

As in past years, SLO posts abroad faced increasing workloads related to immigration screening requirements. As a result, CSIS Headquarters provided temporary assistance and relief to certain SLO posts to assist with screening backlogs.

FEDERAL COURT WARRANTS AND WARRANT STATISTICS

Warrants are one of the most powerful and intrusive tools available. They provide CSIS with Federal Court authorization to use investigative techniques that would otherwise be illegal, such as monitoring of telephone communications. For this reason, the use of warrants by CSIS deserves continued scrutiny—a task that SIRC takes very seriously.

Each year, SIRC collects statistics on the Service's warrant applications and on warrants granted by the Federal Court. Though SIRC does not have the resources to examine all warrants granted to the Service by the Federal Court, it will look at a certain number of warrants as part of its annual reviews.

When SIRC examines a warrant, it looks into all aspects of the warrant process, starting with the development of the warrant application. SIRC verifies whether:

- CSIS's justification for requesting warrant powers was reasonable;
- CSIS complied with the applicable legal and policy requirements in applying for warrant powers; and
- the warrant application accurately reflected the information held by CSIS.

SIRC also looks at the actual warrant approved by the Federal Court and what happens after that approval (i.e., how the warrant powers were used by CSIS).

Warrant application refers to the process by which CSIS submits warrant requests for consideration by the Service's Warrant Review Committee, the Minister of Public Safety and the Federal Court.

Warrants are documents issued by a Federal Court judge under Section 21(3), 22 or 23 of the *CSIS Act*, authorizing the Service to implement specific powers against particular individuals.

Table 9
Warrant statistics

	2003–04	2004–05	2005–06
New	68	40	24
Replaced or renewed	130	207	203
Total	198	247	227

During the period under review, 24 new warrants were approved by the Federal Court. It also approved the renewal or replacement of 203 warrants. Included among the 227 warrants were 31 urgent warrants approved in 2005–06: more than three times the number approved in the previous year. In 2005–06, there were 248 expired or terminated warrants, compared to 220 in the previous fiscal year.

The Service also reported judicial decisions in 2005–06 that affected its applications for warrants, the execution of powers contained in warrants, or the warrant process generally. In two cases, the Court did not approve warrant powers. In the first instance, the judge decided that although the activities of the individual clearly constituted a threat to the security of Canada, the granting of warrant powers was premature. In the second instance, the judge refused the application on factual grounds. On other applications, the Federal Court requested additional information and clarification before approving the warrants. It also requested that the Service submit interim reports on the execution of certain warrant powers to ensure they were used for the purposes intended.

During 2005–06, the Federal Court dismissed an application for warrants. The decision was based on the fact that the Service had not provided full, fair and accurate disclosure of all material facts in the affidavit. The Court's decision was without prejudice to the right of the Service to bring forward a new application in relation to the same targets.

The Service subsequently provided the Court with a full explanation of the circumstances in question, and at that time, also informed the Minister of Public Safety, SIRC and the Office of the Inspector General. As a precautionary measure, the Director imposed a moratorium on the filing of warrant applications with the Federal Court until he was satisfied, on a case by case basis, that the Service's disclosure obligations had been addressed.

The Director has instigated a full review of the warrant process under the leadership of the Service's General Counsel. This request stemmed from his concerns about efficacy, timeliness and accountability of the current procedures, as the warrant application process has become increasingly complex and cumbersome over recent years. The implementation of the recommendations of the warrant review, which is scheduled for Fall 2006, is subject to consultation with the Department of Justice and the Department of Public Safety.

Moreover, since the dismissal of the warrant application, CSIS's Director and General Counsel have appeared before a Federal Court panel to discuss the case and the process for preparing and submitting warrant applications.

Also of note, although Section 28 of the *CSIS Act* authorizes the Governor-in-Council to make regulations governing the forms of warrants, practices and procedures applicable to the application hearings, as well as the location and manner in which hearings may be held, there were no such regulations made during this or any previous review period.

INTEGRATED THREAT ASSESSMENT CENTRE

For details on the Centre's mandate and how it operates, see *Review of the Integrated Threat Assessment Centre (# 2005-03)* in this annual report. During 2005-06, ITAC issued 98 threat assessments and redistributed 382 others that were produced by the fusion centres of allied intelligence agencies. ITAC was also responsible for advising the National Security Advisor to the Prime Minister concerning several special threat assessments.

The majority of ITAC staff are seconded from partner agencies for a period of two years. Seconded staff are subject to the *CSIS Act* in the same fashion as CSIS employees. Despite being operational for two years, ITAC was not fully staffed at the end of the period under review.

Section 3

Want to know more about SIRC?

Want to know more about SIRC?

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Gary Filmon, P.C., O.M., who was appointed on June 24, 2005. The other Members are the Honourable Raymond Speaker, P.C., O.C., the Honourable Baljit S. Chadha, P.C., the Honourable Roy Romanow, P.C., O.C., Q.C., and the Honourable Aldéa Landry, P.C., C.M., Q.C.

All Members of SIRC are Privy Councillors, who are appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties.

SIRC provides assurance to Parliament—and through it, to Canadians—that CSIS complies with legislation, policy and Ministerial Direction in the performance of its duties and functions. SIRC seeks to ensure that the Service does not undermine the fundamental rights and freedoms of Canadians. It is the only independent, external body equipped with the legal mandate and expertise to review the activities of CSIS. Moreover, SIRC is a cornerstone of Canada's democratic tradition as it ensures the accountability of one of the government's most powerful organizations.

In addition to attending monthly committee meetings, members preside over complaints hearings, prepare reviews and complaint reports in consultation with SIRC staff, visit CSIS regional offices, appear before Parliament and exercise other duties associated with their responsibilities.

SIRC meetings and briefings 2005–06

April 18, 2005: SIRC's Executive Director addressed the Special Senate Committee reviewing the *Anti-Terrorism Act*.

May 11, 2005: SIRC staff participated in the first Review Agencies Forum, attended by representatives of the Office of the Commissioner of the Communications Security Establishment (CSE) and the Inspector General of CSIS.

May 17, 2005: SIRC's Executive Director and senior staff met with officials from the United Kingdom's Intelligence and Security Committee.

May 18–19, 2005: SIRC co-hosted the International Symposium on Review and Oversight, together with its partner, the Canadian Centre of Intelligence and Security Studies of Carleton University.

May 20, 2005: The Executive Director and senior staff met with officials of the Dutch Supervisory Committee for Intelligence and Security Services.

May 31, 2005: SIRC met with the Independent Advisor to the Minister of Public Safety, regarding Air India.

June 7, 2005: The Executive Director and senior staff met with their counterparts from the O'Connor Commission concerning its policy review.

June 8, 2005: The Associate Executive Director and Senior Counsel addressed the Special House Committee reviewing the *Anti-Terrorism Act*.

August 22, 2005: The Executive Director and senior staff met with their counterparts from the O'Connor Commission concerning its policy review.

Continued on the next page

SIRC meetings and briefings 2005–06

(continued)

October 6, 2005: The Executive Director attended a Queen's University-Government of Canada policy seminar in Kingston on Canada-U.S. relations regarding the security environment.

October 11, 2005: The Executive Director was a guest lecturer at Carleton University's Canadian Centre of Intelligence and Security Studies graduate seminar on intelligence, statecraft and international affairs.

October 20–22, 2005: The Executive Director and staff attended the annual conference of the Canadian Association of Security and Intelligence Studies in Montreal.

November 17, 2005: SIRC's Chair and Executive Director appeared at a public hearing of the O'Connor Commission, concerning its policy review.

November 18, 2005: The Executive Director was a guest lecturer at a Carleton University political science course entitled "Oversight and Access."

December 2, 2005: The Associate Executive Director made a presentation to an international seminar in Brasilia, Brazil, on intelligence and the democratic state.

December 12, 2005: The Executive Director and senior staff met with their counterparts from the O'Connor Commission concerning its policy review.

January 24, 2006: SIRC hosted the second Review Agencies Forum, attended by representatives of the Office of the Commissioner of the CSE, the Inspector General of CSIS, and the Commission for Public Complaints Against the RCMP.

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Susan Pollak, and a staff of 19, located in Ottawa. The staff comprises: an Associate Executive Director, a Deputy Executive Director, Senior Counsel, a Corporate Services Manager, Counsel, a Senior Paralegal (who also serves as Access to Information and Privacy Officer/Analyst), four administrative staff, and nine researchers.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

As part of their ongoing work, the Chair of SIRC, Committee Members, and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of the security intelligence community.

These exchanges are supplemented by discussions with academics, security and intelligence experts and relevant non-governmental organizations, such as human rights groups. Such activities enrich SIRC's knowledge about issues and opinions affecting the security intelligence field.

SIRC also visits CSIS regional offices on a rotating basis to examine how Ministerial Direction and CSIS policy affect the day-to-day work of investigators in the field. These trips give Committee Members an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. It is also an opportunity to communicate SIRC's focus and concerns.

Continued on the next page

During the 2005–06 fiscal year, SIRC visited two regional offices. Over the last five years, SIRC has visited all six CSIS regional offices. In addition, SIRC staff received specialized training in a regional office concerning investigative techniques used by the Service. See *SIRC meetings and briefings 2005–06* for a summary of additional activities undertaken by SIRC during this period.

BUDGET AND EXPENDITURES

SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures. Table 10 below presents a breakdown of actual and estimated expenditures.

INQUIRIES UNDER THE ACCESS TO INFORMATION AND PRIVACY ACTS

The public may make requests to SIRC under both the *Access to Information Act* and the *Privacy Act*. Table 11 outlines the number of requests SIRC has received under these acts for the past three fiscal years.

SIRC meetings and briefings 2005–06

(continued)

March 3, 2006: The Executive Director of SIRC and members of the Canadian Centre of Intelligence and Security Studies (Council of Advisors and Executive Committee) attended an international conference, entitled "Critical Energy Infrastructure Protection Policy: Assessing Threats, Vulnerabilities and Responses."

March 15, 2006: The Executive Director was the guest lecturer at a Dalhousie University graduate seminar in Halifax, entitled "Parliamentary Oversight of the Canadian Security Intelligence Service."

March 21, 2006: The Executive Director and senior staff met with the United Kingdom's Joint Parliamentary Committee on Human Rights.

Table 10
SIRC expenditures 2005–06

	2005–06 (Actual)	2005–06 (Estimates)
Personnel	\$1,796,000	\$1,777,000
Goods and services	\$941,702	\$1,019,000
Total	\$2,737,702	\$2,796,000

Access to Information requests for SIRC's studies represent the largest portion of access requests. SIRC waives the application fees for all such requests.

Table 11
Requests for release of information

	2003–04	2004–05	2005–06
<i>Access to Information Act</i>	31	21	17
<i>Privacy Act</i>	1	3	5

COMMUNICATIONS

To commemorate its 20th anniversary, SIRC co-hosted a major international symposium with the Canadian Centre of Intelligence and Security Studies of Carleton University. Held in May 2005, the theme of this two-day event was “Making National Security Accountable: International Perspectives on Intelligence Review and Oversight,” which was explored in panel discussions and keynote speeches. The symposium attracted over 200 registered delegates and featured a range of experts from both Canada and abroad.

Although SIRC's annual report is the main communications vehicle for informing Parliament and Canadians about its work, it has implemented a modest communications program. SIRC has also undertaken some public opinion research, which shows that Canadians' awareness of review bodies remains very low, although perceptions of their independence and objectivity remain positive.

SIRC's website is continually updated with information relevant to the security and intelligence community. Since the website was first launched, traffic has

increased significantly, with the number of “total successful requests” more than doubling, to 539,789 in April 2006, from 201,267 a year ago.

SIRC posted an Arabic translation of “How to Make a Complaint” on its website in January 2006.

In an effort to be inclusive and to ensure that its recourse mechanism is well-understood, SIRC posted an Arabic translation of “How to Make a Complaint” on its website in January 2006. In addition, CSIS’s home page now features a direct hyperlink to SIRC’s website. As principal spokesperson, the Chair has met with some journalists to discuss SIRC’s work, and is scheduled to deliver several speeches in the upcoming year.

MODERN COMPTROLLERSHIP

In 2005–06, SIRC contracted for an independent audit of its policy framework to confirm that its policies and procedures were consistent with Treasury Board requirements. It also aimed to identify gaps or omissions requiring attention. Moreover, SIRC developed competency profiles for all its staff and completed position descriptions for its researchers and counsel.

In the coming year, SIRC will be implementing an improved financial management framework, which will introduce further rigor to the way resources are allocated and expenditures are monitored. The Report on Plans and Priorities is the foundation on which budgets for SIRC’s program activities and priorities are established.

Also of note, SIRC contracted for an independent financial audit, which will examine how SIRC has used additional resources that were approved earlier by Parliament. This audit was completed in June 2006.

Appendix A

SIRC reviews since 1984

SIRC reviews since 1984

Note: Reviews flagged with an “*” are Section 54 reports, which are special documents SIRC prepares for the Minister of Public Safety.

1. *Eighteen Months After Separation: An Assessment of CSIS Approach to Staffing Training and Related Issues* (SECRET) (86/87-01)*
2. *Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service* (SECRET) (86/87-02)*
3. *The Security and Intelligence Network in the Government of Canada: A Description* (SECRET) (86/87-03)*
4. *Ottawa Airport Security Alert* (SECRET) (86/87-05)*
5. *Report to the Solicitor General of Canada Concerning CSIS Performance of its Functions* (SECRET) (87/88-01)*
6. *Closing the Gaps: Official Languages and Staff Relations in the CSIS* (UNCLASSIFIED) (86/87-04)*
7. *Counter-Subversion: SIRC Staff Report* (SECRET) (87/88-02)
8. *SIRC Report on Immigration Screening* (SECRET) (87/88-03)*
9. *Report to the Solicitor General of Canada on CSIS Use of Its Investigative Powers with Respect to the Labour Movement* (PUBLIC VERSION) (87/88-04)*
10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process* (SECRET) (88/89-01)*
11. *SIRC Review of the Counter-Terrorism Program in the CSIS* (TOP SECRET) (88/89-02)*
12. *Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS* (SECRET) (89/90-02)*
13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement* (SECRET) (89/90-03)*

14. *A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information* (SECRET) (89/90-04)
15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information* (SECRET) (89/90-05)*
16. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons* (UNCLASSIFIED) (89/90-06)
17. *SIRC Report on the Innu Interview and the Native Extremism Investigation* (SECRET) (89/90-07)*
18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988* (SECRET) (89/90-01)*
19. *A Review of the Counter-Intelligence Program in the CSIS* (TOP SECRET) (89/90-08)*
20. *Domestic Exchanges of Information* (SECRET) (90/91-03)*
21. *Section 2(d) Targets—A SIRC Study of the Counter-Subversion Branch Residue* (SECRET) (90/91-06)
22. *Regional Studies* (six studies relating to one region) (TOP SECRET) (90/91-04)
23. *Study of CSIS Policy Branch* (CONFIDENTIAL) (90/91-09)
24. *Investigations, Source Tasking and Information Reporting on 2(b) Targets* (TOP SECRET) (90/91-05)
25. *Release of Information to Foreign Agencies* (TOP SECRET) (90/91-02)*
26. *CSIS Activities Regarding Native Canadians—A SIRC Review* (SECRET) (90/91-07)*
27. *Security Investigations on University Campuses* (TOP SECRET) (90/91-01)*
28. *Report on Multiple Targeting* (SECRET) (90/91-08)
29. *Review of the Investigation of Bull, Space Research Corporation and Iraq* (SECRET) (91/92-01)

30. *Report on Al Mashat's Immigration to Canada* (SECRET) (91/92-02)*
31. *East Bloc Investigations* (TOP SECRET) (91/92-08)
32. *Review of CSIS Activities Regarding Sensitive Institutions* (TOP SECRET) (91/92-10)
33. *CSIS and the Association for New Canadians* (SECRET) (91/92-03)
34. *Exchange of Information and Intelligence between CSIS & CSE, Section 40* (TOP SECRET) (91/92-04)*
35. *Victor Ostrovsky* (TOP SECRET) (91/92-05)
36. *Report on Two Iraqis—Ministerial Certificate Case* (SECRET) (91/92-06)
37. *Threat Assessments, Section 40 Study* (SECRET) (91/92-07)*
38. *The Attack on the Iranian Embassy in Ottawa* (TOP SECRET) (92/93-01)*
39. "STUDYNT" *The Second CSIS Internal Security Case* (TOP SECRET) (91/92-15)
40. *Domestic Terrorism Targets—A SIRC Review* (TOP SECRET) (90/91-13)*
41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations* (TOP SECRET) (91/92-18)
43. *CSIS Activities during the Gulf War: Community Interviews* (SECRET) (90/91-12)
44. *Review of CSIS Investigation of a Latin American Illegal* (TOP SECRET) (90/91-10)*
45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985—A SIRC Review* (TOP SECRET) (91/92-14)*
46. *Prairie Region—Report on Targeting Authorizations (Chapter 1)* (TOP SECRET) (90/91-11)*

47. *The Assault on Dr. Hassan Al-Turabi* (SECRET) (92/93–07)
48. *Domestic Exchanges of Information (A SIRC Review—1991/92)* (SECRET) (91/92–16)
49. *Prairie Region Audit* (TOP SECRET) (90/91–11)
50. *Sheik Rahman's Alleged Visit to Ottawa* (SECRET) (CT 93–06)
51. *Regional Audit* (TOP SECRET)
52. *A SIRC Review of CSIS SLO Posts (London & Paris)* (SECRET) (91/92–11)
53. *The Asian Homeland Conflict* (SECRET) (CT 93–03)
54. *Intelligence-Source Confidentiality* (TOP SECRET) (CI 93–03)
55. *Domestic Investigations (1)* (SECRET) (CT 93–02)
56. *Domestic Investigations (2)* (TOP SECRET) (CT 93–04)
57. *Middle East Movements* (SECRET) (CT 93–01)
58. *A Review of CSIS SLO Posts (1992-93)* (SECRET) (CT 93–05)
59. *Review of Traditional CI Threats* (TOP SECRET) (CI 93–01)
60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93–04)
61. *Domestic Exchanges of Information* (SECRET) (CI 93–05)
62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93–06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 93–11)
64. *Sources in Government* (TOP SECRET) (CI 93–09)
65. *Regional Audit* (TOP SECRET) (CI 93–02)
66. *The Proliferation Threat* (SECRET) (CT 93–07)

67. *The Heritage Front Affair. Report to the Solicitor General of Canada* (SECRET) (CT 94-02)*
68. *A Review of CSIS' SLO Posts (1993-94)* (SECRET) (CT 93-09)
69. *Domestic Exchanges of Information (A SIRC Review 1993-94)* (SECRET) (CI 93-08)
70. *The Proliferation Threat—Case Examination* (SECRET) (CT 94-04)
71. *Community Interviews* (SECRET) (CT 93-11)
72. *An Ongoing Counter-Intelligence Investigation* (TOP SECRET) (CI 93-07)*
73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)
74. *A SIRC Review of CSIS SLO Posts (1994-95)* (SECRET) (CT 95-01)
75. *Regional Audit* (TOP SECRET) (CI 93-10)
76. *Terrorism and a Foreign Government* (TOP SECRET) (CT 94-03)
77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)
78. *Review of Certain Foreign Intelligence Services* (TOP SECRET) (CI 94-02)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 94-01)
80. *Domestic Exchanges of Information (A SIRC Review 1994-95)* (SECRET) (CI 94-03)
81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)
82. *CSIS and a "Walk-In"* (TOP SECRET) (CI 95-04)
83. *A Review of a CSIS Investigation Relating to a Foreign State* (TOP SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 95-05)

85. *Regional Audit* (TOP SECRET) (CT 95–02)
86. *A Review of Investigations of Emerging Threats* (TOP SECRET) (CI 95–03)
87. *Domestic Exchanges of Information* (SECRET) (CI 95–01)
88. *Homeland Conflict* (TOP SECRET) (CT 96–01)
89. *Regional Audit* (TOP SECRET) (CI 96–01)
90. *The Management of Human Sources* (TOP SECRET) (CI 96–03)
91. *Economic Espionage I* (SECRET) (CI 96–02)
92. *Economic Espionage II* (TOP SECRET) (CI 96–02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996–97* (TOP SECRET) (CI 96–04)
94. *Urban Political Violence* (SECRET) (SIRC 1997–01)
95. *Domestic Exchanges of Information (1996–97)* (SECRET) (SIRC 1997–02)
96. *Foreign Conflict—Part I* (SECRET) (SIRC 1997–03)
97. *Regional Audit* (TOP SECRET) (SIRC 1997–04)
98. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1997–05)
99. *Spy Case* (TOP SECRET) (SIRC 1998–02)
100. *Domestic Investigations (3)* (TOP SECRET) (SIRC 1998–03)
101. *CSIS Cooperation with the RCMP—Part I* (SECRET) (SIRC 1998–04)*
102. *Source Review* (TOP SECRET) (SIRC 1998–05)
103. *Interagency Cooperation Case* (TOP SECRET) (SIRC 1998–06)
104. *A Case of Historical Interest* (TOP SECRET) (SIRC 1998–08)

105. *CSIS Role in Immigration Security Screening* (SECRET) (CT 95-06)
106. *Foreign Conflict—Part II* (TOP SECRET) (SIRC 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)
108. *CSIS Cooperation with the RCMP—Part II* (SECRET) (SIRC 1998-04)*
109. *Audit of Section 16 Investigations & Foreign Intelligence 1997-98*
(TOP SECRET) (SIRC 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)
111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)
113. *Allegations by a Former CSIS Employee* (TOP SECRET) (SIRC 1998-12)*
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET)
(SIRC 1998-15)
116. *Files* (TOP SECRET) (SIRC 1998-16)
117. *Audit of Section 16 Investigations & Foreign Intelligence* (TOP SECRET)
(SIRC 1999-01)
118. *A Long-Running Counter Intelligence Investigation* (TOP SECRET)
(SIRC 1999-02)
119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)
120. *Proliferation* (TOP SECRET) (SIRC 1999-04)
121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—
Bill C-31* (PROTECTED) (SIRC 1999-05)*
122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)

123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999–07)
124. *Regional Audit* (TOP SECRET) (SIRC 1999–08)
125. *Foreign State Activities* (TOP SECRET) (SIRC 1999–09)
126. *Project Sidewinder* (TOP SECRET) (SIRC 1999–10)*
127. *Security Breach* (TOP SECRET) (SIRC 1999–11)
128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET)
(SIRC 2000–01)
129. *Audit of Section 16 Investigations and Foreign Intelligence Reports
1999–2000* (TOP SECRET) (SIRC 2000–02)
130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000–03)
131. *Regional Audit* (TOP SECRET) (SIRC 2000–04)
132. *Warrant Review* (TOP SECRET) (SIRC 2000–05)
133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000*
(TOP SECRET (SIRC 2001–02)
134. *CSIS Investigation of Sunni Islamic Extremism* (TOP SECRET)
(SIRC 2002–01)
135. *Source Recruitment* (TOP SECRET) (SIRC 2001–01)
136. *Collection of Foreign Intelligence* (TOP SECRET) (SIRC 2001–05)
137. *Domestic Extremism* (TOP SECRET) (SIRC 2001–03)
138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TOP SECRET)
(SIRC 2001–04)
139. *Warrant Review* (TOP SECRET) (SIRC 2001–06)
140. *Special Report following allegations pertaining to an individual*
(TOP SECRET)*

141. *Audit of Section 16 and Foreign Intelligence Reports* (TOP SECRET) (SIRC 2002-02)
142. *Review of the Ahmed Ressam Investigation* (TOP SECRET) (SIRC 2002-03)
143. *Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the Anti-Globalization Movement* (TOP SECRET) (SIRC 2002-04)
144. *Regional Audit* (TOP SECRET) (SIRC 2002-05)
145. *Special Report (2002-2003) following allegations pertaining to an individual* (TOP SECRET)*
146. *Front End Screening Program* (TOP SECRET) (SIRC 2003-01)
147. *CSIS Section 12 Operational Activity Outside Canada* (TOP SECRET) (SIRC 2003-02)
148. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2003-03)
149. *Review of a Counter-Proliferation Investigation* (TOP SECRET) (SIRC 2003-04)
150. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2003-05)
151. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2004-01)
152. *Review of CSIS's Investigation of Transnational Criminal Activity* (TOP SECRET) (SIRC 2004-02)
153. *Review of the Terrorist Entity Listing Process* (SECRET) (SIRC 2004-03)
154. *Review of Activities and Investigations in a CSIS Regional Office* (TOP SECRET) (SIRC 2004-04)
155. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2004-05)

156. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2004–06)
157. *Review of CSIS's Investigation of Threats against Canada's Critical Information Infrastructure* (TOP SECRET) (SIRC 2004–07)
158. *Review of CSIS's Exchanges of Information with Close Allies* (TOP SECRET) (SIRC 2004–08)
159. *Review of a Counter-Proliferation Investigation* (TOP SECRET) (SIRC 2004–09)
160. *Terrorist Financing Activities in Canada* (TOP SECRET) (SIRC 2004–10)
161. *Section 54 Report to the Minister of Public Safety and Emergency Preparedness* (TOP SECRET)*
162. *Review of a counter-terrorism investigation* (TOP SECRET) (SIRC 2005–01)
163. *CSIS liaison with foreign agencies: review of a security liaison post* (TOP SECRET) (SIRC 2005–02)
164. *Review of the Integrated Threat Assessment Centre* (TOP SECRET) (SIRC 2005–03)
165. *Review of a counter-intelligence investigation* (TOP SECRET) (SIRC 2005–04)
166. SIRC is currently working on this review, but it had not been finalized at the time this annual report went to print (SIRC 2005–05)
167. *Review of foreign arrangements with countries suspected of human rights violations* (TOP SECRET) (SIRC 2005–06)
168. *Review of CSIS's electronic-surveillance and information-gathering techniques* (TOP SECRET) (SIRC 2005–07)
169. *Review of activities and investigations in a CSIS region* (TOP SECRET) (SIRC 2005–08)

Appendix B

Recommendations

Recommendations

During 2005–06, SIRC made 14 recommendations stemming from the reviews it conducted. These recommendations are summarized below.

Review	SIRC recommended that...
# 2005-01	<ul style="list-style-type: none"> • CSIS extend its sensitive sector policy to require senior-level approval for certain investigative techniques.
# 2005-02	<ul style="list-style-type: none"> • CSIS Security Liaison Officers should maintain a written record when requests for information from CSIS Headquarters are transmitted verbally to foreign intelligence agencies. • CSIS update the post profile. • CSIS Headquarters remind operational branches and SLOs to submit reports [of discussions with foreign partners] in a timely fashion. • CSIS produce an assessment document concerning a new relationship with a specific foreign agency, especially since CSIS Headquarters made the same request in 2003. • CSIS develop an operational policy for documenting its relationships with agencies that are known or reputed to have engaged in human-rights abuse.
# 2005-03	<ul style="list-style-type: none"> • CSIS review its policies to determine where ITAC-specific amendments are required to address the role of this organization. • CSIS formalize its relationship with [another foreign fusion centre] and seek an approved foreign arrangement from the Minister of Public Safety.

Review	SIRC recommended that...
# 2005-06	<ul style="list-style-type: none"> • CSIS amend its policy governing the disclosure of information to foreign agencies, to include consideration of the human rights record of the country and possible abuses by its security or intelligence agencies. • CSIS Headquarters should maintain a written record of secure telephone conversations with SLOs—specifically conversations that contain operational information—and include this in its reporting. • CSIS review its procedures so that the parameters and methods of exchange—as well as the Service’s expectations—are communicated to the foreign agency prior to entering into new foreign arrangements.
# 2005-07	<ul style="list-style-type: none"> • CSIS review and revise the warrant policy in question so that it reflects current best practices.
# 2005-08	<ul style="list-style-type: none"> • CSIS obtain an updated legal opinion governing the use of [a certain interception] technique. • Existing operational policy [concerning internal security measures] be strictly adhered to by all regions, regardless of location, size or staff complement.

Le CSARS a recommandé...		Examen
<ul style="list-style-type: none">• Que le SCRS modifie sa politique sur la communication d'information à des organismes étrangers de manière à prévoir la prise en compte de la réputation des pays intéressés, au chapitre des droits de la personne, et des violations possibles de la part de leurs services de sécurité ou de renseignement.• Que l'Administration centrale du SCRS tienne un compte rendu des conversations téléphoniques protégées avec les ALS, en particulier de celles contenant des renseignements opérationnels, et que ce compte rendu figure dans ses rapports.• Que le SCRS revioie sa procédure de manière à communiquer aux organismes étrangers les paramètres et les méthodes d'échange, de même que ses attentes, avant de conclure de nouvelles ententes avec eux.		N° 2005-06
<ul style="list-style-type: none">• Que le SCRS examine et retouche la politique en question sur les mandats afin qu'elle reflète les pratiques exemplaires actuelles.		N° 2005-07
<ul style="list-style-type: none">• Que [le SCRS] obtienne une opinion juridique à jour sur l'emploi [d'une] technique [d'interception] particulière.• Que tous les bureaux régionaux se conforment strictement à la politique opérationnelle en place [concernant les mesures de sécurité interne], quels que soient l'endroit où ils sont situés ainsi que leur taille ou leur effectif.		N° 2005-08

Au cours de l'exercice 2005-2006, le CSARS a formulé 14 recommandations découlant des examens qu'il a effectués. Voici le résumé de ces recommandations.

Examen		Le CSARS a recommandé...
N° 2005-01	<ul style="list-style-type: none">• Que le SCRS élargisse sa politique relative aux secteurs névral- giques de manière à exiger que certaines techniques d'enquête soient autorisées par la haute direction.	
N° 2005-02	<ul style="list-style-type: none">• Que les agents de liaison-sécurité du SCRS conservent par écrit les demandes d'information de l'Administration centrale du SCRS qu'ils transmettent verbalement aux services de renseignement étrangers.• Que le SCRS mette à jour le profil du bureau.• Que l'Administration centrale du SCRS rappelle aux directions opérationnelles et aux ALS de présenter [les] rapports [de discussions avec des partenaires] promptement.• Que le SCRS établisse un document d'évaluation d'une nouvelle relation avec un organisme étranger donné, en particulier parce que l'Administration centrale du SCRS avait formulé la même requête en 2003.• Que le SCRS élabore une politique opérationnelle concernant la documentation de ses relations avec les organismes qui sont connus pour leurs violations des droits de la personne ou auxquels on attribue de tels gestes.	
N° 2005-03	<ul style="list-style-type: none">• Que le SCRS examine ses politiques pour déterminer les modifications particulières qui s'imposent à l'égard du CLEM afin de tenir compte du rôle de cet organisme.• Que le SCRS officialise sa relation avec [un autre centre de fusion étranger] et fasse approuver une entente par le ministre de la Sécurité publique.	

Annexe B

Recommendations

155. *Review of a Counter Terrorism Investigation* (TRÈS SECRET) (SIRC 2004-05)
156. *Review of a Counter Intelligence Investigation* (TRÈS SECRET) (SIRC 2004-06)
157. *Review of CSIS's Investigation of Threats against Canada's Critical Information Infrastructure* (TRÈS SECRET) (SIRC 2004-07)
158. *Review of CSIS's Exchanges of Information with Close Allies* (TRÈS SECRET) (SIRC 2004-08)
159. *Review of a Counter-Proliferation Investigation* (TRÈS SECRET) (SIRC 2004-09)
160. *Terrorist Financing Activities in Canada* (TRÈS SECRET) (SIRC 2004-10)
161. *Section 54 Report to the Minister of Public Safety and Emergency Preparedness* (TRÈS SECRET)*
162. *Review of a counter-terrorism investigation* (TRÈS SECRET) (SIRC 2005-01)
163. *CSIS liaison with foreign agencies: review of a security liaison post* (TRÈS SECRET) (SIRC 2005-02)
164. *Review of the Integrated Threat Assessment Centre* (TRÈS SECRET) (SIRC 2005-03)
165. *Review of a counter-intelligence investigation* (TRÈS SECRET) (SIRC 2005-04)
166. Le CSARS travaille actuellement à cette étude qui n'était toutefois pas finalisée au moment de mettre sous presse (SIRC 2005-05)
167. *Review of foreign arrangements with countries suspected of human rights violations* (TRÈS SECRET) (SIRC 2005-06)
168. *Review of CSIS's electronic-surveillance and information-gathering techniques* (TRÈS SECRET) (SIRC 2005-07)
169. *Review of activities and investigations in a CSIS region* (TRÈS SECRET) (SIRC 2005-08)

140. Rapport spécial sur des allégations concernant une personne (TRÈS SECRET)*
141. Audit of Section 16 and Foreign Intelligence Reports (TRÈS SECRET)
(SIRC 2002-02)
142. Review of the Ahmed Ressam Investigation (TRÈS SECRET) (SIRC 2002-03)
143. Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the
Anti-Globalization Movement (TRÈS SECRET) (SIRC 2002-04)
144. Regional Audit (TRÈS SECRET) (SIRC 2002-05)
145. Rapport spécial (2002-2003) sur des allégations concernant une personne
(TRÈS SECRET)*
146. Front End Screening Program (TRÈS SECRET) (SIRC 2003-01)
147. CSIS Section 12 Operational Activity Outside Canada (TRÈS SECRET)
(SIRC 2003-02)
148. Review of a Counter Intelligence Investigation (TRÈS SECRET)
(SIRC 2003-03)
149. Review of a Counter Proliferation Investigation (TRÈS SECRET)
(SIRC 2003-04)
150. CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post
(TRÈS SECRET) (SIRC 2003-05)
151. CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post
(TRÈS SECRET) (SIRC 2004-01)
152. Review of CSIS's Investigation of Transnational Criminal Activity
(TRÈS SECRET) (SIRC 2004-02)
153. Review of the Terrorist Entity Listing Process (SECRET) (SIRC 2004-03)
154. Review of Activities and Investigations in a CSIS Regional Office
(TRÈS SECRET) (SIRC 2004-04)

139. *Warrant Review* (TRÈS SECRET) (SIRC 2001-06)
138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TRÈS SECRET) (SIRC 2001-04)
137. *Domestic Extremism* (TRÈS SECRET) (SIRC 2001-03)
136. *Collection of Foreign Intelligence* (TRÈS SECRET) (SIRC 2001-05)
135. *Source Recruitment* (TRÈS SECRET) (SIRC 2001-01)
134. *CSIS Investigation of Sunni Islamic Extremism* (TRÈS SECRET) (SIRC 2002-01)
133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999-2000* (TRÈS SECRET) (SIRC 2001-02)
132. *Warrant Review* (TRÈS SECRET) (SIRC 2000-05)
131. *Regional Audit* (TRÈS SECRET) (SIRC 2000-04)
130. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 2000-03)
129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999-2000* (TRÈS SECRET) (SIRC 2000-02)
128. *Domestic Exchanges of Information 1999-2000* (TRÈS SECRET) (SIRC 2000-01)
127. *Security Breach* (TRÈS SECRET) (SIRC 1999-11)
126. *Le Projet Sidewinder* (TRÈS SECRET) (SIRC 1999-10)*
125. *Foreign State Activities* (TRÈS SECRET) (SIRC 1999-09)
124. *Regional Audit* (TRÈS SECRET) (SIRC 1999-08)
123. *Terrorist Fundraising* (TRÈS SECRET) (SIRC 1999-07)

107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)
108. *Coopération du SCRS avec la GRC – partie II* (SECRET) (SIRC 1998-04)*
109. *Audit of Section 16 Investigations and Foreign Intelligence 1997-98* (TRÈS SECRET) (SIRC 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)
111. *Regional Audit* (TRÈS SECRET) (SIRC 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 1998-11)
113. *Allégations d'un ancien employé du SCRS* (TRÈS SECRET) (CSARS 1998-12)*
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TRÈS SECRET) (SIRC 1998-15)
116. *Files* (TRÈS SECRET) (SIRC 1998-16)
117. *Audit of Section 16 Investigations and Foreign Intelligence* (TRÈS SECRET) (SIRC 1999-01)
118. *A Long-Running Counter Intelligence Investigation* (TRÈS SECRET) (SIRC 1999-02)
119. *Domestic Exchanges of Information* (TRÈS SECRET) (SIRC 1999-03)
120. *Proliferation* (TRÈS SECRET) (SIRC 1999-04)
121. *Observations du CSARS sur le projet de loi C-31 dont est actuellement saisi le Parlement* (PROTÉGÉ) (SIRC 1999-05)*
122. *Domestic Targets* (TRÈS SECRET) (SIRC 1999-06)

90. *La gestion des sources humaines* (TRÈS SECRET) (CE 96-03)
91. *Economic Espionage I* (SECRET) (CI 96-02)
92. *Economic Espionage II* (TRÈS SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996-1997* (TRÈS SECRET) (CI 96-04)
94. *Urban Political Violence* (SECRET) (SIRC 1997-01)
95. *Domestic Exchanges of Information (1996-97)* (SECRET) (SIRC 1997-02)
96. *Conflit étrangers, partie I* (SECRET) (SIRC 1997-03)
97. *Regional Audit* (TRÈS SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 1997-05)
99. *Spy Case* (TRÈS SECRET) (SIRC 1998-02)
100. *Enquêtes menées au Canada (3)* (TRÈS SECRET) (CSARS 1998-03)
101. *Coopération du SCRS avec la Gendarmerie royale du Canada – partie I* (SECRET) (CSARS 1998-04)*
102. *Source Review* (TRÈS SECRET) (SIRC 1998-05)
103. *Interagency Cooperation Case* (TRÈS SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest* (TRÈS SECRET) (SIRC 1998-08)
105. *Le rôle du SCRS dans le filtrage de sécurité des demandes d'immigration* (SECRET) (CT 95-06)
106. *Un conflit étrangers, partie II* (TRÈS SECRET) (SIRC 1997-03)

73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)
74. *A SIRC Review of CSIS' SLO Posts (1994-95)* (SECRET) (CT 95-01)
75. *Regional Audit* (TRÈS SECRET) (CI 93-10)
76. *Terrorism and a Foreign Government* (TRÈS SECRET) (CT 94-03)
77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)
78. *Review of Certain Foreign Intelligence Services* (TRÈS SECRET) (CI 94-02)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 94-01)
80. *Echanges d'information avec des organismes canadiens (enquête du CSARS 1994-1995)* (SECRET) (CI 94-03)
81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)
82. *CSIS and a "Walk-In"* (TRÈS SECRET) (CI 95-04)
83. *A Review of a CSIS Investigation relating to a Foreign State* (TRÈS SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 95-05)
85. *Vérification régionale* (TRÈS SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats* (TRÈS SECRET) (CI 95-03)
87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)
88. *Homeland Conflict* (TRÈS SECRET) (CT 96-01)
89. *Vérification régionale* (TRÈS SECRET) (CI 96-01)

56. *Enquêtes menées au Canada (2)* (TRÈS SECRET) (CT 93-04)
57. *Middle East Movements* (SECRET) (CT 93-01)
58. *A Review of CSIS' SLO Posts (1992-93)* (SECRET) (CT 93-05)
59. *Review of Traditional CI Threats* (TRÈS SECRET) (CI 93-01)
60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)
61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)
62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 93-11)
64. *Sources in Government* (TRÈS SECRET) (CI 93-09)
65. *Regional Audit* (TRÈS SECRET) (CI 93-02)
66. *The Proliferation Threat* (SECRET) (CT 93-07)
67. *L'Affaire du Héritage Front, rapport présenté au Solliciteur général du Canada* (SECRET) (AT 94-02)*
68. *A Review of CSIS' SLO Posts (1993-94)* (SECRET) (CT 93-09)
69. *Échanges d'information avec des organismes canadiens (enquête du CSARS 1993-1994)* (SECRET) (CI 93-08)
70. *The Proliferation Threat – Case Examination* (SECRET) (CT 94-04)
71. *Community Interviews* (SECRET) (CT 93-11)
72. *Une enquête suivie en matière de contre-espionnage* (TRÈS SECRET) (CE 93-07)*

41. CSIS Activities with respect to Citizenship Security Screening (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations* (TRÈS SECRET) (91/92-18)
43. *Activités du SCRS pendant la Guerre du Golfe : entrevues dans la communauté* (SECRET) (90/91-12)
44. *Examen de l'enquête menée par le SCRS sur un agent clandestin latino-américain – un examen du CSARS* (TRÈS SECRET) (90/91-10)*
45. *Les activités du SCRS relativement à la destruction de l'avion affecté au vol 182 d'Air India le 23 juin 1985 – un examen du CSARS* (TRÈS SECRET) (91/92-14)*
46. *Région des Prairies – rapport sur les autorisations d'enquête (chapitre 1)* (TRÈS SECRET) (90/91-11)*
47. *L'attentat contre Hassan El-Tourabi* (SECRET) (92/93-07)
48. *Domestic Exchanges of Information (A SIRC Review – 1991/92)* (SECRET) (91/92-16)
49. *Vérification de la région des Prairies* (TRÈS SECRET) (90/91-11)
50. *La présumée venue du sheikh Rahman à Ottawa* (SECRET) (CT 93-06)
51. *Regional Audit* (TRÈS SECRET)
52. *Examen par le CSARS des bureaux des ALS du Service (Londres et Paris)* (SECRET) (91/92-11)
53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)
54. *Intelligence-Source Confidentiality* (TRÈS SECRET) (CI 93-03)
55. *Domestic Investigations (1)* (SECRET) (CT 93-02)

26. Examen par le CSARS des activités du SCRS touchant les Canadiens autochtones (SECRET) (90/91-07)*
27. Enquêtes de sécurité sur les campus universitaires (TRÈS SECRET) (90/91-01)*
28. Report on Multiple Targeting (SECRET) (90/91-08)
29. Revue de l'enquête sur Bull, la Corporation de recherche spatiale et l'Iraq (SECRET) (91/92-01)
30. Rapport sur l'immigration d'Al Mashat au Canada (SECRET) (91/92-02)*
31. East Bloc Investigations (TRÈS SECRET) (91/92-08)
32. Review of CSIS Activities Regarding Sensitive Institutions (TRÈS SECRET) (91/92-10)
33. CSIS and the Association for New Canadians (SECRET) (91/92-03)
34. Échange d'informations et de renseignements entre le Service canadien du renseignement de sécurité et le Centre de la sécurité des télécommunications (TRÈS SECRET) (91/92-04)*
35. Victor Ostrovsky (TRÈS SECRET) (91/92-05)
36. Report on Two Iraqis – Ministerial Certificate Case (SECRET) (91/92-06)
37. Évaluations de la menace, étude en vertu de l'article 40 (SECRET) (91/92-07)*
38. L'attaque contre l'ambassade de l'Iran à Ottawa (TRÈS SECRET) (92/93-01)*
39. "STUDYNT" The Second CSIS Internal Security Case (TRÈS SECRET) (91/92-15)
40. Les cibles du terrorisme national – un examen du CSARS (TRÈS SECRET) (90/91-13)*

12. Rapport présenté au Solliciteur général du Canada sur la protection des biens scientifiques et techniques au Canada : le rôle du SCRS (SECRET) (89/90-02)*
13. SIRC Report on CSIS Activities Regarding the Canadian Peace Movement (SECRET) (89/90-03)*
14. Examen de la politique et des pratiques du SCRS concernant les divulgations non autorisées d'informations classifiées (SECRET) (89/90-04)
15. Report to the Solicitor General of Canada on Citizenship/Third Party Information (SECRET) (89/90-05)*
16. Modifications à la Loi sur le SCRS : propositions au Comité spécial de la Chambre des communes (NON CLASSIFIÉ) (89/90-06)
17. Rapport sur l'entrevue concernant les Innus et l'enquête sur l'extrémisme autochtone (SECRET) (89/90-07)*
18. Supplement to the Committee's Report on Immigration Screening of January 18, 1988 (SECRET) (89/90-01)*
19. A Review of the Counter-Intelligence Program in the CSIS (TRÈS SECRET) (89/90-08)*
20. Échanges de renseignements avec des organismes canadiens (SECRET) (90/91-03)*
21. Cibles établies en vertu de l'alinéa 2d) – une étude du CSARS sur les opérations restantes de la Direction de l'antisubversion (SECRET) (90/91-06)
22. Études régionales (six études sur une région) (TRÈS SECRET) (90/91-04)
23. Study of CSIS' Policy Branch (CONFIDENTIEL) (90/91-09)
24. Enquêtes, affectation de sources et rapport sur les cibles en vertu de l'alinéa 2b) (TRÈS SECRET) (90/91-05)
25. Communication de renseignements aux services étrangers (TRÈS SECRET) (90/91-02)*

Examens du CSARS depuis 1984

Nota : les rapports marqués d'un astérisque (*) sont des documents spéciaux que le CSARS prépare à l'intention du ministre de la Sécurité publique en vertu de l'article 54.

1. Dix-huit mois après la séparation : une appréciation de la conception du SCRS sur le recrutement, le perfectionnement et les questions connexes (SECRET) (86/87-01)*
2. Rapport d'une étude portant sur le filtrage de sécurité des fonctionnaires et des personnes postulant un emploi dans la fonction publique fédérale (SECRET) (86/87-02)*
3. Le réseau du renseignement et de sécurité au sein de l'administration gouvernementale du Canada : une description (SECRET) (86/87-03)*
4. Alerie de sécurité à l'aéroport d'Ottawa (SECRET) (86/87-05)*
5. Report to the Solicitor General of Canada Concerning CSIS Performance of its Functions (SECRET) (87/88-01)*
6. Pour corriger une situation : langues officielles et relations de travail au sein du SCRS (NON CLASSIFIÉ) (86/87-04)*
7. Counter-Subversion: SIRC Staff Report (SECRET) (87/88-02)
8. Rapport du CSARS – Sélection des immigrants (SECRET) (87/88-03)*
9. L'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrier (VERSION PUBLIQUE) (87/88-04)*
10. La Direction de l'évaluation du renseignement : une revue par le CSARS du processus de production (SECRET) (88/89-01)*
11. CSARS – Examen du programme de l'antiterrorisme du SCRS (TRÈS SECRET) (88/89-02)*

Annexe A

Examens du CSARS depuis 1984

La CSARS a affiché sur son site Web, en janvier 2006, une traduction arabe de sa procédure intitulée « Comment porter plainte ».

Dans le but de mieux répondre aux besoins et d'assurer que son mécanisme de recours est bien compris, le CSARS a affiché sur son site Web, en janvier 2006, une traduction arabe de sa procédure intitulée « Comment porter plainte ». De plus, la page d'accueil du site Web du SCRS comporte maintenant un lien hypertextuel menant directement au site Web du Comité. En qualité de premier porte-parole, le président a rencontré quelques journalistes pour leur exposer les travaux du CSARS et il doit prononcer plusieurs allocutions au cours du prochain exercice.

FONCTION DE CONTRÔLEUR MODERNE

En 2005-2006, le CSARS a imparté la vérification indépendante de son cadre stratégique afin de confirmer la conformité de ses politiques et procédures aux exigences du Conseil du Trésor. Cette vérification visait aussi à relever les lacunes ou omissions requérant son attention. Le Comité a aussi élaboré des profils de compétences pour tout son personnel et des descriptions de poste pour ses chercheurs et avocats.

Au cours du prochain exercice, le CSARS instaurera un cadre de gestion financière améliorée qui confèrera plus de rigueur au mode d'affectation des ressources et de contrôle des dépenses. Le Rapport sur les plans et priorités est le document sur lequel est fondée la budgétisation des activités de programme et des priorités du CSARS.

Il importe en outre de signaler que le CSARS a confié en sous-traitance une vérification comptable indépendante. Ce travail, qui a pris fin en juin 2006, portait sur l'usage que le Comité avait fait des crédits supplémentaires approuvés par le Parlement.

Le gros des demandes d'accès à l'information concernent des études du Comité. Celui-ci ne perçoit aucun droit pour l'ensemble de ces demandes.

Tableau 11

Demandes de communication de renseignements

		2003-2004		2004-2005		2005-2006	
Loi sur l'accès à l'information		31		21		17	
Loi sur la protection des renseignements personnels		1		3		5	

COMMUNICATIONS

Pour commémorer son 20^e anniversaire, le Comité a tenu un important colloque international avec le Canadian Centre of Intelligence and Security Studies de l'Université Carleton. Cette rencontre de deux jours, qui a eu lieu en mai 2005, avait pour thèmes la responsabilisation en matière de sécurité nationale et les perspectives internationales en matière de surveillance et de contrôle du renseignement. Ces questions ont été examinées dans le cadre de discussions de groupe et de discours liminaires. Le colloque a attiré plus de 200 délégués inscrits et regroupé un éventail d'experts canadiens et étrangers.

Même s'il fait de son rapport annuel le principal moyen d'informer le Parlement et les Canadiens de ses travaux, le Comité n'en a pas moins mis en œuvre un modeste programme de communication. Il a en outre mené, en matière d'opinion publique, des recherches dont les résultats montrent que les Canadiens sont encore très peu sensibilisés à la question des organismes de surveillance, quoique les perceptions quant à l'indépendance et à l'objectivité de ceux-ci demeurent positives.

Le CSARS renouvelle constamment l'information affichée sur son site Web au sujet de la collectivité de la sécurité et du renseignement. Depuis l'inauguration du site, le nombre de visiteurs a augmenté de façon considérable, le nombre de demandes pleinement fructueuses ayant plus que doublé et atteignant 539 789 en avril 2006, de 201 267 qu'il était un an plus tôt.

Réunions et séances
d'information du CSARS,
2005-2006

(suite)

24 janvier 2006 : le CSARS tient le second Forum des organismes de surveillance auquel prennent part des représentants du Bureau du commissaire du CST, de l'inspecteur général du SCRS et de la Commission des plaintes du public contre la GRC.

3 mars 2006 : le directeur exécutif du CSARS et des membres du Canadian Centre of Intelligence and Security Studies (Conseil consultatif et Comité exécutif) assistent à une conférence internationale sur la politique de protection des infrastructures énergétiques essentielles et l'évaluation des menaces, des vulnérabilités et des réponses.

15 mars 2006 : le directeur exécutif est conférencier invité à un séminaire d'études supérieures de l'Université Dalhousie, à Halifax, sur la surveillance du Service canadien du renseignement de sécurité par le Parlement.

21 mars 2006 : le directeur exécutif et des cadres supérieurs rencontrent le Comité parlementaire mixte du Royaume-Uni sur les droits de la personne.

Au cours de 2005-2006, les membres du Comité se sont rendus dans deux bureaux régionaux du SCRS. Les cinq derniers exercices les avaient amenés dans six de ces bureaux. De plus, dans l'un d'eux, le personnel du Comité a reçu une formation spécialisée dans les techniques d'enquête employées par le Service. Voir *Réunions et séances d'information du CSARS, 2005-2006*, qui résume les autres activités menées par le Comité durant cette période.

BUDGET ET DÉPENSES

Le Comité continue de gérer ses activités dans les limites des ressources qui lui sont octroyées. Ses principales dépenses ont trait au traitement de son personnel et à leurs déplacements au Canada pour prendre part aux audiences, aux séances d'information et aux activités d'examen du Comité. Le tableau 10 présente une ventilation des dépenses réelles et des prévisions à ce chapitre.

DEMANDES EN VERTU DES LOIS SUR L'ACCÈS
À L'INFORMATION ET SUR LA PROTECTION DES
RENSEIGNEMENTS PERSONNELS

Le public peut présenter au CSARS des demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. Le tableau 11 fait état du nombre de demandes que ces lois ont values au Comité au cours des trois derniers exercices.

Tableau 10
Dépenses du CSARS 2005-2006

2005-2006 (dépenses réelles)	2005-2006 (prévisions)
Personnel	1 777 000 \$
Biens et services	1 019 000 \$
Total	2 796 000 \$

PERSONNEL ET ORGANISATION

Le Comité jouit du soutien de son directeur exécutif, Susan Pollak, et d'un effectif de 19 employés, en poste à Ottawa. Son personnel est ainsi composé : un directeur exécutif associé, un sous-directeur exécutif, un avocat principal, un directeur des services généraux, un avocat, un parajuriste principal (aussi agent/analyste à l'accès à l'information et à la protection des renseignements personnels), quatre employés de soutien administratif et neuf chercheurs.

Les membres du Comité dicent au personnel l'orientation à donner aux travaux de recherche et autres activités qui sont désignées prioritaires pour l'année. La marche des affaires courantes est confiée au directeur exécutif qui s'enquiert au besoin de la ligne de conduite à tenir auprès du président, premier dirigeant du CSARS.

Dans le cadre de leurs travaux suivis, le président et les membres du Comité ainsi que les cadres supérieurs prennent part à des discussions régulières avec la direction et le personnel du SCRS et avec d'autres membres de haut rang de la collectivité du renseignement de sécurité. À ces échanges se greffent des discussions avec des universitaires, des experts du renseignement et de la sécurité et des organismes non gouvernementaux compétents, tels des groupes de défense des droits de la personne. Ces activités visent à enrichir les connaissances du CSARS au sujet des dossiers et opinions qui intéressent le domaine du renseignement de sécurité.

Les membres du Comité visitent aussi les bureaux régionaux du Service à tour de rôle pour examiner l'incidence des instructions ministérielles et de la politique du SCRS sur le travail courant des enquêteurs locaux. Ces visites leur fournissent l'occasion d'entendre les cadres régionaux du Service leur exposer les problèmes, difficultés et priorités propres à ces bureaux. Elles leur permettent aussi de faire valoir ce qui polarise les efforts et les préoccupations du CSARS.

Réunions et séances d'information du CSARS, 2005-2006

(suite)

22 août 2005 : le directeur exécutif et des cadres supérieurs rencontrent leurs homologues de la Commission O'Connor au sujet de son examen stratégique.

6 octobre 2005 : le directeur exécutif assiste, à Kingston, à un séminaire de haut niveau tenu par l'Université Queen's et le gouvernement du Canada, sur les relations canado-américaines en ce qui a trait au contexte de la sécurité.

11 octobre 2005 : le directeur exécutif donne une conférence sur le renseignement, l'habileté politique et les affaires internationales, à titre d'invité à un séminaire d'études supérieures tenu par le Canadian Centre of Intelligence and Security Studies à l'Université Carleton.

20-22 octobre 2005 : le directeur exécutif et des membres du personnel assistent à la conférence annuelle de l'Association canadienne pour l'étude de la sécurité et du renseignement, à Montréal.

17 novembre 2005 : le président et le directeur exécutif du CSARS comparassent à une audience publique de la Commission O'Connor au sujet de son examen stratégique.

18 novembre 2005 : le directeur exécutif est conférencier invité à un cours de science politique de l'Université Carleton sur le contrôle et l'accès.

2 décembre 2005 : le directeur exécutif associé fait un exposé sur le renseignement et l'État démocratique, à un séminaire international tenu à Brasília, au Brésil.

12 décembre 2005 : le directeur exécutif et des cadres supérieurs rencontrent leurs homologues de la Commission O'Connor au sujet de son examen stratégique.

Suite sur la prochaine page

COMPOSITION DU COMITÉ

La présidence du Comité est occupée par l'honorable Gary Filmon, C.P., O.M., nommé à cette charge le 24 juin 2005. Les autres membres sont l'honorable Raymond Speaker, C.P., O.C., l'honorable Baljit S. Chadha, C.P., l'honorable Roy Romanow, C.P., O.C., c.r., et l'honorable Aldéa Landry, C.P., C.M., c.r.

Tous les membres du Comité font partie du Conseil privé et sont nommés par le gouverneur en conseil après consultation entre le premier ministre et les chefs des partis de l'opposition.

Le Comité fournit au Parlement, et par son entremise aux Canadiens, l'assurance que le SCRS respecte la loi, les politiques et les instructions ministérielles dans l'exercice de ses fonctions. Il veille à ce que le Service ne sape pas les droits fondamentaux et les libertés des Canadiens. Le CSARS est le seul organisme indépendant, de l'extérieur, à être habilité par la loi et à avoir l'expertise voulue pour surveiller les activités du SCRS. De plus, il est la pierre angulaire de la tradition démocratique canadienne, car il assure la reddition de comptes de l'un des organismes gouvernementaux les plus puissants.

En plus d'assister aux réunions mensuelles du Comité, les membres président les audiences de plaintes, préparent les rapports d'examen et de plaintes en consultation avec le personnel du CSARS, visitent les bureaux régionaux du SCRS, compareraissent devant le Parlement et exercent d'autres fonctions liées à leurs responsabilités.

Réunions et séances d'information du CSARS, 2005-2006

18 avril 2005 : le directeur exécutif du CSARS prend la parole devant le Comité sénatorial spécial sur la teneur de la Loi antiterroriste.

11 mai 2005 : le personnel du CSARS participe au premier Forum des organismes de surveillance auquel prennent part des représentants du Bureau du commissaire du Centre de la sécurité des télécommunications (CST) et de l'inspecteur général du SCRS.

17 mai 2005 : le directeur exécutif et des cadres supérieurs du Comité rencontrent des représentants du Comité du renseignement et de la sécurité du Royaume-Uni.

18-19 mai 2005 : le CSARS tient un colloque international sur la surveillance et le contrôle, avec son partenaire, le Canadian Centre of Intelligence and Security Studies de l'Université Carleton.

20 mai 2005 : le directeur exécutif et des cadres supérieurs rencontrent des représentants du Comité hollandais de surveillance des services de renseignement et de sécurité.

31 mai 2005 : le Comité rencontre le conseiller indépendant auprès du ministre de la Sécurité publique, au sujet d'Air India.

7 juin 2005 : le directeur exécutif et des cadres supérieurs rencontrent leurs homologues de la Commission O'Connor au sujet de son examen stratégique.

8 juin 2005 : le directeur exécutif associé et l'avocate principale prennent la parole devant le Comité spécial de la Chambre sur la teneur de la Loi antiterroriste.

Section 3

Voulez-vous en savoir plus long
sur le CSARS?

De plus, depuis le rejet de la demande de mandat, le directeur et l'avocat général du Service ont comparu devant un groupe de la Cour fédérale afin de discuter de l'affaire ainsi que du processus de préparation et de présentation des demandes de mandat.

Il importe aussi de noter que l'article 28 de la *Loi sur le SCRS* autorise le gouverneur en conseil à établir des règlements applicables aux formes des mandats, aux pratiques et à la procédure applicables à l'audition des demandes ainsi qu'aux lieux où les audiences peuvent être tenues et à la forme qu'elles peuvent prendre. Aucun règlement semblable n'a été établi, ni pendant la période étudiée ni au cours des précédentes.

CENTRE INTÉGRÉ D'ÉVALUATION DES MENACES

Pour plus de détails sur le mandat et le mode de fonctionnement du Centre intégré d'évaluation des menaces (CIEM), voir l'étude *Examen du Centre intégré d'évaluation des menaces (no 2005-03)*, dans le présent rapport annuel. Au cours de 2005-2006, le CIEM a fourni 98 évaluations de la menace et en a redistribué 382 autres émanant de centres de fusion rattachés à des services de renseignement alliés. Le CIEM était aussi chargé d'aviser le conseiller à la sécurité nationale auprès du premier ministre au sujet de plusieurs évaluations spéciales de la menace.

La majeure partie des membres du personnel du CIEM sont détachés pour deux ans par des organismes partenaires. Les intéressés sont assujettis à la *Loi sur le SCRS* au même titre que les employés du Service. L'effectif du CIEM n'était pas complet à la fin de la période à l'étude, même si celui-ci était alors opérationnel depuis deux ans.

Au cours de la période étudiée, la Cour fédérale a approuvé 24 mandats nouveaux. Elle a aussi approuvé le renouvellement ou le remplacement de 203 mandats. Parmi ces 227 mandats, 31 étaient des mandats urgents approuvés en 2005-2006, soit plus de trois fois le nombre approuvé durant l'exercice précédent. En 2005-2006, 248 mandats ont pris fin ou ont été révoqués, par rapport à 220 pendant l'exercice précédent.

Le Service a aussi fait état de décisions judiciaires qui, en 2005-2006, ont eu une incidence sur ses demandes de mandats, sur l'exercice des pouvoirs octroyés par ceux-ci ou sur le processus des mandats en général. Dans deux cas, la Cour n'a pas approuvé les pouvoirs demandés. Dans le premier cas, le juge a statué que, même si les activités de l'individu visé constituaient une menace manifeste envers la sécurité du Canada, il était prématuré d'octroyer des pouvoirs par un mandat. Dans le second cas, le juge a rejeté la requête pour des motifs d'ordre factuel. À l'égard d'autres demandes, la Cour fédérale a demandé des renseignements supplémentaires et des éclaircissements avant d'approuver les mandats. Elle a aussi demandé au Service de présenter des rapports provisoires sur l'exercice de certains pouvoirs visés dans les mandats pour s'assurer que ces pouvoirs servaient aux fins prévues.

Au cours de 2005-2006, la Cour fédérale a rejeté une demande de mandats, fondant sa décision sur le fait que le SCRS n'avait pas divulgué de façon complète, impartiale et exacte tous les faits pertinents dans l'affidavit. Cette décision ne portait pas préjudice au droit du Service de présenter une nouvelle demande à l'égard des mêmes cibles.

Le Service a par la suite fourni à la Cour des explications complètes sur les circonstances en question et, à ce moment-là, il a également informé le ministre de la Sécurité publique, le CSARS et le Bureau de l'inspecteur général. Par mesure de précaution, le directeur a imposé un moratoire sur la présentation de demandes de mandats à la Cour fédérale jusqu'à ce qu'il soit convaincu, dans chaque cas, que le Service avait rempli ses obligations en matière de divulgation.

Le directeur a amorcé un examen complet du processus des demandes de mandats, sous la direction de l'avocat général du Service. Cette démarche découlait du fait qu'il s'interrogeait sur l'efficacité et la rapidité de la procédure existante, et sur la reddition de comptes à cet égard, ce processus étant devenu de plus en plus complexe et lourd ces dernières années. La mise en œuvre des recommandations découlant de cette étude, qui est prévue pour l'automne 2006, est assujettie à la consultation du ministère de la Justice et du ministère de la Sécurité publique.

MANDATS DE LA COUR FÉDÉRALE : GÉNÉRALITÉS ET STATISTIQUES

Mis à part leur caractère fort intrusif, les mandats sont l'un des instruments les plus puissants. Ils procurent au SCRS l'autorisation de la Cour fédérale à employer des méthodes d'enquête qui seraient autrement illégales, par exemple l'interception de communications téléphoniques. Pour cette raison, le recours aux mandats par le Service justifie une surveillance constante, tâche que le Comité prend très au sérieux.

Chaque année, le CSARS recueille des statistiques sur les demandes de mandats du Service et sur les mandats que la Cour fédérale lui décerne. Il n'a pas les ressources voulues pour examiner tous les mandats octroyés par la Cour fédérale, mais il en étudie un certain nombre dans le cadre de ses examens annuels.

Lorsque le CSARS examine un mandat, il étudie tous les éléments du processus des mandats, se penchant d'abord sur l'élaboration de la demande. Il vérifie si :

- les raisons fournies par le SCRS pour justifier les pouvoirs demandés sont raisonnables;
- le SCRS s'est conformé aux exigences applicables sur le plan de la loi et des politiques en demandant de se faire conférer des pouvoirs par la voie d'un mandat ;
- la demande de mandat reflète fidèlement l'information dont disposait le SCRS.

Le SCRS examine aussi le mandat même, décerné par la Cour fédérale, et ce qui s'est passé par la suite (c.-à-d., la manière dont le SCRS a exercé les pouvoirs qui lui avaient été octroyés).

Tableau 9
Statistiques sur les mandats

	2003-2004	2004-2005	2005-2006
Mandats nouveaux	68	40	24
Mandats remplacés ou renouvelés	130	207	203
Total	198	247	227

L'EDI est un réseau électronique qui sert à présenter les demandes de filtrage et qui vise à en réduire le temps de traitement. Plus de 50 clients ministériels recourent à ce service, de sorte que la presque totalité des demandes de candidats au statut de réfugié, à l'immigration ou à la citoyenneté sont reçues par cette voie. Comme lors de précédents exercices, le SCRS a signalé au CSARS qu'il avait continué d'étendre l'accès à l'EDI à d'autres clients au cours de l'exercice, dont six nouveaux clients ministériels et deux nouveaux bureaux d'immigration.

DIRECTION DE LA LIAISON AVEC L'ÉTRANGER ET DES VISITES

La Direction de la liaison avec l'étranger et des visites (LEV) assure la liaison du Service avec des organismes étrangers et coordonne les visites de représentants étrangers à l'Administration centrale du SCRS et à ses bureaux régionaux. Elle est aussi chargée de coordonner toutes les ententes conclues en vertu du paragraphe 17(1) avec des services étrangers de renseignement de sécurité ou de maintien de l'ordre, de même que le fonctionnement des bureaux de liaison-sécurité à l'extérieur du pays.

À la fin de 2005-2006, le Service était partie à un total de 265 ententes avec des organismes de 144 pays. Pendant cette période, le Ministère l'a autorisé à en conclure six nouvelles, à en modifier ou en améliorer quatre autres et à en suspendre trois.

De ces 265 ententes avec des organismes étrangers, 217 étaient actives, 39 inappliquées (se dit d'une absence de liaison pendant au moins un an) et 9 suspendues ou restreintes (y compris les 3 mentionnées au paragraphe précédent). Toute entente dite « inappliquée » ou « restreinte » demeure telle tant qu'il n'y a pas eu d'évaluation à jour des relations.

La Direction de la LEV est aussi chargée des bureaux de liaison-sécurité auxquels le Service confie les rapports avec les services de sécurité et de renseignement étrangers. Les agents de liaison-sécurité sont aussi appelés à évaluer l'efficacité de chacune des ententes conclues en vertu de l'article 17 avec des organismes étrangers et à présenter une évaluation annuelle de la fiabilité de chacun de ceux-ci à titre de partenaire, et de sa réputation au chapitre des droits de la personne. Pour de plus amples renseignements, voir *Liaison du SCRS avec des organismes étrangers : examen d'un bureau de liaison-sécurité (n° 2005-02)*, dans le présent rapport annuel.

Comme par les années passées, la charge de travail des bureaux d'ALS à l'étranger n'a cessé de s'alourdir en ce qui touche le filtrage des demandes d'immigration. Aussi l'Administration centrale du SCRS a-t-elle affecté temporairement des employés à certains bureaux d'ALS pour les aider à éliminer l'arrière de filtrage.

Le tableau 8 fait état des données triennales sur les délais médians du Service à fournir des avis de vérification de données.

Tableau 8
Délais médians (en jours) à fournir des avis de vérification de données

	2003-2004	2004-2005	2005-2006
Citoyenneté	1	1	1
Demandes d'immigration, au Canada	46	44	70
Demandes d'immigration, à l'étranger	5	7	16
Demandes d'immigration, aux États-Unis	152	150	62
Détermination du statut de réfugié	53	56	96
Contrôle de sécurité préliminaire	32	27	23
Filtrage des demandes de visa	12	13	11

Autres activités de filtrage – En 2005-2006, la Direction du filtrage de sécurité a étudié plus de 36 000 demandes de visa de ressortissants étrangers. Elle a aussi commencé à participer au programme Expéditions rapides et sécuritaires (EXPRES) et fait plus de 3 000 évaluations de sécurité de camionneurs qui avaient demandé un laissez-passer frontalier en vertu de ce programme. Pour plus de renseignements sur celui-ci, prière de consulter le site de l'Agence des services frontaliers du Canada à www.cbsa-asfc.gc.ca/import/fast/menu-f.html.

Autres programmes – Les Programmes de contrôle de sécurité préliminaire (PCSP) et d'échange de données informatisées (EDI) ont été créés en 2001 pour faciliter les processus de filtrage des candidats à l'immigration et au statut de réfugié. Le PCSP vise à vérifier toutes les demandes de candidats au statut de réfugié par rapport aux dossiers du SCRS afin de repérer ceux qui pourraient poser des risques relatifs à la sécurité, et cela, le plus rapidement possible dans le processus de détermination du statut de réfugié. D'autres renseignements sur le Programme d'EDI figurent dans l'étude n° 2003-01 du CSARS, qui est résumée dans son rapport annuel de 2003-2004.

Tableau 7
Types de demandes de filtrage à l'immigration

	Demandes*					Avis	
	2003-2004	2004-2005	2005-2006	2003-2004	2004-2005	2004-2005	2005-2006
Au Canada et à l'étranger	57 300	56 100	63 200	106	88	133	
Contrôle de sécurité préliminaire**	22 700	22 900	17 100	92	184	89	
Détermination du statut de réfugié***	16 500	14 200	11 700	122	110	127	
Total partiel	96 500	93 200	92 000	320	382	349	
Demandes de citoyenneté	203 400	161 200	308 000	150	124	120	
Total	299 900	254 400	400 000	470	506	469	

* Chiffres arrondis à la centaine la plus proche.

** Représente les personnes qui demandent le statut de réfugié à l'arrivée à la frontière canadienne.

*** Représente les réfugiés (au sens de la LIPR) qui demandent, au Canada même, le statut de résident permanent.

la grande majorité de ses enquêtes de filtrage de candidats au statut de réfugié, à l'immigration ou à la citoyenneté – il n'en trouve que pour 1 demande sur 250 de candidats à l'immigration ou au statut de réfugié et pour 1 demande de citoyenneté sur 2 500. En 2005-2006, pour l'ensemble des avis relatifs au filtrage à l'immigration (349), le SCRS a remis 232 notes d'information et 117 avis de non-admissibilité. On recense aussi 12 lettres d'aneccdotc.

Le CSARS a noté qu'en général les délais du Service à remettre des notes d'information ou des avis de non-admissibilité sont assez longs. Pour les notes d'information concernant les dossiers d'immigration, ils sont de 12 à 18 mois, selon la provenance de la demande. Pour les dossiers de réfugiés, le délai médian a été de 10 mois pour ce qui est du Programme de contrôle de sécurité préliminaire. Le CSARS a relevé des délais médians semblables en ce qui touche les avis de non-admissibilité. Pour les dossiers d'immigration, le délai d'exécution a été de 12 à 18 mois et, pour ceux des candidats au statut de réfugié, il a été de 8 à 11 mois.

Les avis du SCRS concernant le filtrage de sécurité peuvent prendre l'une ou l'autre des cinq formes suivantes : (suite)

- 3. **Note d'information :** remise dans les cas de filtrage pour le gouvernement si le SCRS découvre des informations qui pourraient influencer la décision de l'organisme demandeur d'octroyer à un candidat une habilitation de sécurité ou d'accès à des sites. Aussi remise dans les cas de filtrage à l'immigration si le Service a des informations voulant que le candidat trempe ou ait trempé dans des activités qui ne le rendent pas nécessairement interdit de territoire au Canada.
- 4. **Avis de non-admissibilité :** fourni à CIC ou à l'ASFC si le demandeur est réputé interdit de territoire au Canada, selon les dispositions de la LIPR relatives à la sécurité.
- 5. **Avis de refus :** remis dans les cas où le Service recommande à un organisme demandeur qu'une habilitation de sécurité ou d'accès à des sites soit refusée au candidat.

Filtrage à l'immigration – La Direction du filtrage de sécurité du SCRS mène aussi des enquêtes et conseille Citoyenneté et Immigration Canada et l'Agence des services frontaliers du Canada pour appuyer le traitement des demandes de candidats au statut de réfugié ainsi qu'à l'immigration et à la citoyenneté. Le Service tient ses pouvoirs à cet égard des articles 14 et 15 de la *Loi sur le SCRS*.

En 2005-2006, la Direction a reçu quelque 92 000 demandes en vertu des divers programmes de filtrage à l'immigration (voir le tableau 7), soit un peu moins que lors des exercices précédents. On note une forte baisse (de près de 20 p. 100) dans le nombre des demandes de filtrage de candidats au statut de réfugié par rapport à l'exercice précédent, alors que le nombre des demandes de citoyenneté a presque doublé. Il importe aussi de noter une hausse d'environ 13 p. 100 du nombre des demandes de filtrage à l'immigration.

Selon le tableau qui précède, le SCRS ne trouve aucun renseignement défavorable dans

Tableau 6 Programmes de filtrage concernant l'accès à des sites*

	2003-2004			2004-2005			2005-2006		
	Total								
Cité parlementaire	1 400			1 100			1 000		
Accès aux zones réglementées d'aéroports	28 800			31 100			37 600		
Centrales nucléaires	5 700			6 800			10 600		
Expéditions rapides et sécuritaires (EXPRES)	s.o.			21 500**			3 100		
Accréditation en vue d'événements spéciaux	0			1 800			5 600		
Autres ministères	1 400			2 300			2 400		
	37 300			64 600			60 300		

* Chiffres arrondis à la centaine la plus proche.

** Vise une demande spéciale d'examen de laissez-passer octroyés antérieurement, donnant suite à une aggravation des craintes en matière de sécurité relativement à l'élection présidentielle américaine.

Les avis du SCRS concernant le filtrage de sécurité peuvent prendre l'une ou l'autre des cinq formes suivantes :

1. **Avis de vérification des données :** remis dans les cas de filtrage concernant le gouvernement et l'immigration si le Service ne trouve aucun renseignement défavorable au sujet du demandeur.
2. **Lettre d'anecdote :** fournie à Citoyenneté et Immigration Canada (CIC) et à l'Agence des services frontaliers du Canada (ASFC) si le Service a des renseignements au sujet d'un demandeur qui prend ou a pris part à des activités étrangères à la sécurité, décrites dans la Loi sur l'immigration et la protection des réfugiés (LIPR).

Pour jauger son efficacité à répondre aux demandes d'habilitations de sécurité, le SCRS calcule les délais d'exécution en nombres médians de jours⁶. Comme le montre le tableau 5, les délais d'exécution médians ont diminué en 2005-2006, en général, par rapport à l'exercice précédent. Le temps de préparation des évaluations de sécurité pour le MDN a diminué sensiblement à tous les niveaux.

Tableau 5
Délais médians (en jours)

	2003-2004			2004-2005			2005-2006		
	Niveau I (Confidentiel)	Niveau II (Secret)	Niveau III (Très secret)	Niveau I (Confidentiel)	Niveau II (Secret)	Niveau III (Très secret)	Niveau I (Confidentiel)	Niveau II (Secret)	Niveau III (Très secret)
MDN	20	18	96	49	63	70	24	19	39
Autres que le MDN				12	14		15	13	60
	Niveau I (Confidentiel)								
	Niveau II (Secret)								

Le Service ne refuse pas, comme telles, les habilitations de sécurité. Il fait plutôt part, au ministre ou à l'organisme demandeur, des renseignements qui l'empêcheraient de recommander l'habilitation. En de rares occasions, le SCRS recommande à l'organisme demandeur de refuser l'habilitation. Il incombe toutefois à celui-ci d'accepter ou de rejeter cette recommandation. En 2005-2006, le Service a présenté 19 notes d'information contenant des renseignements défavorables et il a remis 1 avis de refus.

Le SCRS offre aussi un service de filtrage concernant l'accès à des sites. Contrairement à la core de sécurité du gouvernement, l'autorisation d'accès à des sites permet simplement au titulaire d'accéder à certaines zones protégées à l'intérieur d'installations ou elle l'accrédite en vue d'un événement spécial. En 2005-2006, le SCRS a reçu plus de 60 000 demandes de filtrage de ce type et présenté 4 notes d'information à des organismes demandeurs.

⁶ Le SCRS présente ses statistiques sur les délais de traitement en données médianes, plutôt que moyennes, parce que cette façon de faire atténue l'impact des délais anormalement brefs ou longs et représente mieux le délai de traitement représentatif.

DIRECTION DU FILTRAGE DE SÉCURITÉ

Le programme de l'une des plus grandes directions du SCRS, celle du filtrage de sécurité, comporte deux volets centraux touchant l'un le gouvernement et l'autre, l'immigration.

Filtrage pour le gouvernement – Le SCRS s'occupe des enquêtes de sécurité pour tous les fonctionnaires⁵ qui, dans le cadre de leurs fonctions, doivent avoir accès à des renseignements ou à des biens classifiés. À la suite de chacune de ces enquêtes, il fournit aux ministères et aux organismes demandeurs une évaluation de la loyauté des intéressés envers le Canada en ce qui concerne leur fiabilité personnelle. Les clients qui recourent le plus à ce service sont Travaux publics et Services gouvernementaux Canada et le ministère de la Défense nationale (MDN), regroupant respectivement plus de 25 et 20 p. 100 de toutes les demandes en 2005-2006.

Comme le montre le tableau 4 qui suit, le Service a reçu 42 100 demandes d'habilitations de sécurité nouvelles ou mises à jour en 2005-2006 et il a fourni 37 800 évaluations. Le volume des demandes a augmenté de près de 15 p. 100 par rapport à l'exercice précédent, mais le nombre d'évaluations de sécurité fournies par le SCRS est resté à peu près le même, ce qui montre que celui-ci n'a pu répondre à toutes les demandes en 2005-2006.

Tableau 4

Filtrage pour le gouvernement*

	2003-2004	2004-2005	2005-2006
Demandes du MDN	9 900	9 100	9 200
Demandes d'autres ministères et organismes	27 600	27 400	32 900
Total	37 500	36 500	42 100
Évaluations fournies au MDN	10 100	9 000	8 900
Évaluations fournies aux autres ministères et organismes	27 600	27 600	28 900
Total	37 700	36 600	37 800

* Chiffres arrondis à la centaine la plus proche.

Le SCRS fournit à la GRC des évaluations fondées sur l'information contenue dans ses dossiers, mais il ne mène pas ces enquêtes au nom de la police nationale du Canada. La GRC s'en occupe elle-même.

DIRECTION DE LA RECHERCHE, DE L'ANALYSE ET DE LA PRODUCTION

La Direction de la recherche, de l'analyse et de la production élabore des évaluations du renseignement de sécurité pour appuyer les opérations du Service et la prise de décisions par le gouvernement du Canada relativement aux menaces à la sécurité nationale. Elle effectue des analyses stratégiques et opérationnelles de menaces existantes et de problèmes nouveaux. *Bulletins de renseignements, Rapports du SCRS et Etudes du SCRS* sont les principaux documents qui émanent de cette direction. En 2005-2006, le SCRS a élaboré 41 de ces rapports et les a distribués à l'ensemble de la collectivité du renseignement de sécurité et à d'autres clients.

Comme le CSAARS le mentionnait dans son rapport annuel de 2004-2005, le SCRS a un rôle à jouer dans le processus d'inscription des entités terroristes, dont l'élaboration de rapports de renseignements de sécurité (RRS) qui exposent les motifs de l'inscription d'entités. Ces rapports aident le ministre de la Sécurité publique à décider s'il y a lieu de recommander au gouverneur en conseil d'inscrire une entité particulière sur la liste prévue à cette fin.

En 2005-2006, la Direction a produit neuf RRS. Pendant la même période, elle a aussi entrepris son second examen biennal des RRS existants afin de déterminer s'il est raisonnable de maintenir une entité sur la liste ou de l'en biffer.

Enfin, la Direction appuie les consultations du SCRS auprès d'Affaires étrangères Canada au sujet de l'inscription de noms de personnes ou de groupes à l'annexe I du *Règlement d'application de la résolution des Nations Unies sur la lutte contre le terrorisme*.

Pour de plus amples renseignements sur la liste des entités terroristes, voir le site Web de Sécurité publique à www.psepc-sppcc.gc.ca. Le lecteur est en outre prié de se reporter à l'étude n° 2004-03 du CSAARS, qui est résumée dans le rapport annuel de 2004-2005 du CSAARS.

DIRECTION DE L'ANTITERRORISME

La Direction de l'antiterrorisme a pour rôle de conseiller le gouvernement du Canada au sujet des menaces de violence grave qui pourraient compromettre la sécurité des Canadiens et de leurs alliés.

Pour le cinquième exercice d'affilié, l'extrémisme islamique, notamment celui lié à Al-Qaïda ou sous sa mouvance, demeure la principale préoccupation de cette direction. De plus, le Service estime que la menace que posent ces groupes terroristes s'est aggravée en 2005-2006. L'interdiction de territoire de ces radicaux et leur renvoi du Canada figurent parmi les priorités de la Direction.

Le Service a ouvert plusieurs enquêtes nouvelles sur de présumés extrémistes étrangers ou groupes terroristes qui pouvaient s'être infiltrés au Canada. Il a en outre identifié plusieurs extrémistes canadiens, inconnus jusque-là, qui avaient pris part à des activités liées à la menace. De concert avec d'autres organismes canadiens, la Direction a empêché un présumé extrémiste étranger d'entrer au Canada et elle a neutralisé une cellule terroriste basée au pays.

Nombre des opérations de la Direction de l'antiterrorisme sont menées de concert avec la GRC. Le Service conseille le gouvernement à l'égard des menaces à la sécurité du Canada et la GRC enquête sur la criminalité qui représente une menace semblable. Selon la *Loi antiterroriste* (2001), le rôle de la GRC dans la lutte au terrorisme international a été élargi, ce qui a resserré ses liens avec le SCRS dans les affaires liées à la sécurité nationale. Cela a donné lieu à une collaboration fructueuse en matière de collecte de renseignements et d'opérations techniques.

Le SCRS a signalé au CSARS que, même s'il demeure certains chevauchements entre les enquêtes, chaque organisme s'emploie à régler cette question. En outre, tel que noté dans de précédents rapports annuels, le SCRS fait toujours partie de quatre équipes intégrées de la sécurité nationale de la GRC, situées dans diverses régions du Canada. Ce programme, qui en est à sa cinquième année, doit être implanté dans une cinquième région en 2006.

Les régions participantes du SCRS font état de relations de travail fructueuses avec les équipes. Une coopération étroite et des communications régulières ont limité les chevauchements possibles de mandats entre les deux organismes.

Tableau 3
Cibles autorisées (2005-2006)

Direction	Individus	Organisations	Dossiers/événements	Total	
				192	67
Contre-espionnage	152	36	4	192	67
Lutte contre la prolifération	55	6	6	67	67
Antiterrorisme	274	31	30	335	335
Total	481	73	40	594	594

DIRECTION DE LA LUTTE CONTRE LA PROLIFÉRATION

La Direction de la lutte contre la prolifération enquête sur les activités ayant trait à la prolifération d'armes de destruction massive par les programmes de mise au point et d'acquisition des pays étrangers qui suscitent des inquiétudes ou par ceux d'organisations terroristes. Elle surveille de près les États et groupes voyous qui cautionnent ou commettent des actes terroristes ainsi que les activités des services de renseignements étrangers. La Direction examine en outre la menace que représente le terrorisme chimique, biologique, radiologique et nucléaire.

La Direction a signalé, au niveau de ses enquêtes, divers coups d'éclair qui ont permis au Service de jouer un rôle important dans le partage de renseignements avec ses partenaires étrangers. Elle a en outre élargi ses activités de collecte de renseignements sur le terrorisme d'État et pris part aux efforts du gouvernement du Canada afin de dépister les tentatives pour vider des fonds secrètement à des organisations terroristes internationales.

La Direction de la lutte contre la prolifération a aussi des unités qui prêtent main-forte à d'autres opérations du SCRS. Ce sont, entre autres, la Sous-section des évaluations de la menace (SSEM), qui prépare des rapports d'évaluation sur un vaste éventail de sujets, et la Sous-section de l'évaluation des demandes d'immigration, qui assure la liaison avec l'Agence des services frontaliers du Canada. Les évaluations de la SSEM constituent un mécanisme qui permet d'alerter rapidement le gouvernement au sujet des menaces envers le Canada et les intérêts canadiens à l'étranger. En 2005-2006, la SSEM a effectué 360 évaluations de la menace, contre 450 au cours de l'exercice précédent.

D. Activités opérationnelles du SCRS

Cette section décrit les activités opérationnelles du SCRS et donne un aperçu des priorités et réalisations de chaque direction opérationnelle au cours de 2005-2006. Elle fournit un contexte utile qui guide le CSARS dans la marche de ses propres travaux. Il est bon de mentionner que nombre des unités organisationnelles dont il est question ci-après ont été remodelées par suite de la réorganisation de mai 2006.

DIRECTION DU CONTRE-ESPIONNAGE

La Direction du contre-espionnage axe ses opérations sur les activités hostiles des services de renseignements étrangers que l'on sait à l'œuvre au Canada. Elle enquête sur les menaces à la sécurité nationale, dont l'espionnage et les activités d'inspiration étrangère (p. ex., les efforts pour contrôler, influencer ou manipuler les communautés d'émigrés au Canada). La Direction est aussi chargée d'enquêter sur les menaces à la sécurité de l'économie canadienne, soit l'espionnage économique, l'acquisition clandestine de technologies et la criminalité transnationale. Pour un exemple d'étude du CSARS en ce domaine, voir *Examen d'une enquête de contre-espionnage (n° 2005-04)*, dans le présent rapport annuel.

En 2005-2006, le Service a signalé au CSARS que les activités d'espionnage au Canada se font sans cesse plus complexes et sophistiquées. Cela est particulièrement vrai des cyberattaques et des autres attaques électroniques contre des cibles canadiennes. La Direction a signalé que plusieurs opérations fructueuses avaient été dirigées contre les activités d'espionnage d'un certain nombre d'États étrangers.

Le SCRS a aussi mentionné que les ministères fédéraux invitaient de plus en plus cette direction à présenter ses évaluations et analyses de divers dossiers. Ainsi, la Direction a examiné plus de 80 000 demandes de visa pendant la période étudiée et elle a dépisté un certain nombre d'agents de renseignements connus ou présumés qui cherchaient à entrer au Canada.

INSTRUCTIONS MINISTÉRIELLES

En vertu du paragraphe 6(2) de la *Loi sur le SCRS*, le ministre de la Sécurité publique peut donner des instructions au sujet des activités et enquêtes du Service.

Aucune instruction nouvelle n'a été donnée au cours de l'exercice à l'étude.

Cette issue est conforme avec ce que le CSARS avait prédit dans son rapport annuel de 2000-2001³. À l'époque, il entrevoyait que les instructions ministérielles ne seraient désormais probablement pas mises à jour régulièrement. Le CSARS croyait qu'un accent plus grand sur les politiques opérationnelles propres au Service serait la source des instructions spéciales et des lignes directrices à suivre.

MODIFICATIONS À LA POLITIQUE OPÉRATIONNELLE DU SCRS

La politique opérationnelle du SCRS regroupe les règles qui visent l'éventail des activités constituant son travail. Elle est mise à jour régulièrement selon les modifications législatives et autres. Le Comité étudie tous ces changements pour s'assurer qu'ils respectent la *Loi sur le SCRS*, les instructions ministérielles et les politiques opérationnelles existantes.

En 2005-2006, le SCRS préparait une réorganisation en profondeur de ses opérations, qui a été réalisée en mai 2006. À son avis, un contexte changeant de la menace obligerait à faire ces modifications afin d'intensifier sa capacité opérationnelle, de renforcer et d'appuyer ses activités d'analyse et d'accroître le soutien dans ses rangs⁴.

En 2005-2006, le Service a apporté des modifications à près de 50 politiques, dont 40 traduisant le changement de nom du ministre du Solliciteur général à celui de Sécurité publique et Protection civile Canada. Parmi les autres facteurs qui ont profondément marqué la politique figurent le rôle du SCRS dans l'assistance à l'égard des opérations militaires canadiennes (ce pour quoi il est à élaborer une nouvelle politique) et l'élargissement de sa collecte de renseignements à l'étranger.

RÈGLEMENTS ET NOMINATIONS PAR LE GOUVERNEUR EN CONSEIL

Selon le paragraphe 8(4) de la *Loi sur le SCRS*, le gouverneur en conseil peut établir pour le Service des règlements visant les pouvoirs et fonctions de son directeur ainsi que la conduite et la discipline de ses employés.

Le gouverneur en conseil n'a pris aucun règlement semblable au cours de 2005-2006.

³ *Rapport annuel du CSARS 2000-2001*, page 8.

⁴ Communiqué de presse du SCRS, 1^{er} mai 2006.

En 2005-2006, le CSARS a choisi d'examiner treize ententes conclues avec des organismes de neuf pays.

Le CSARS a constaté que toutes les ententes conclues avec des organismes étrangers étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Le CSARS a aussi constaté que le Service avait pris connaissance de la situation de tous les pays et organismes en question sur le plan des droits de la personne. De plus, le Service avait joué de prudence dans ses échanges d'information avec les pays au bilan doux en matière de respect de ces droits, mais le CSARS n'en continuera pas moins de surveiller une entente particulière.

Même si deux évaluations n'avaient pas été présentées chaque année tel que prescrit, le CSARS a constaté une amélioration dans la présentation annuelle des évaluations et la conformité de l'ensemble de celles-ci aux lignes directrices du Service.

C. Cadre de politiques et de régie

EXIGENCES NATIONALES EN MATIÈRE DE RENSEIGNEMENT DE SÉCURITÉ

Selon le paragraphe 6(2) de la *Loi sur le SCRS*, le ministre de la Sécurité publique peut donner des instructions écrites au directeur du SCRS. Le document intitulé « Exigences nationales en matière de renseignement de sécurité » expose les plans sur lesquels doivent porter les efforts d'enquête du Service et lui dicte les orientations générales à suivre dans l'exercice de ses responsabilités en matière de collecte, d'analyse et de conseil. Ce document est fondé sur un mémoire au Cabinet, que le SCRS prépare chaque année à l'intention du ministre de la Sécurité publique afin qu'il le présente à ses collègues du Cabinet.

En 2005-2006, un mémoire a été examiné et approuvé par le Cabinet, mais il n'y a pas eu d'exigences nationales de publiées. Le Service a informé le CSARS qu'en l'absence d'instructions ministérielles particulières, il s'était fondé sur les priorités approuvées par le Cabinet, qui auraient normalement servi de base aux exigences nationales annuelles.

Le paragraphe 17(1) de la *Loi sur le SCRS* habilite le Service, moyennant autorisation du ministre de la Sécurité publique, à conclure des ententes avec des organismes canadiens ou à collaborer avec eux dans le but d'exercer ses fonctions. Le sous-alinéa 38a)(iii) autorise le Comité à examiner toutes ces ententes.

services de police). Il importe en outre de noter que l'entente conclue en 2004-2005 avec le conseiller à la sécurité nationale a été renouvelée pour une autre année.

ENTENTES AVEC DES ORGANISMES ÉTRANGERS

Selon le paragraphe 17(1) de la *Loi sur le SCRS*, le Service peut conclure des ententes avec des organismes étrangers en vue d'échanger de l'information au sujet de menaces à la sécurité du Canada. Toute nouvelle entente semblable doit être approuvée par le ministre de la Sécurité publique, en consultation avec son homologue des Affaires étrangères. Même en l'absence d'une telle entente, le SCRS peut quand même accepter l'information fournie spontanément par un organisme ou une organisation d'un pays étranger.

Le Service peut aussi élargir le champ des ententes actives, définissant la teneur et l'ampleur des échanges autorisés. Quant aux ententes améliorées, le directeur du SCRS a un pouvoir discrétionnaire plus vaste et il est habilité à approuver une intensification des activités sans obtenir l'autorisation du Ministre, en tenant compte toutefois des mises en garde ou instructions ministérielles qui peuvent avoir été formulées au moment de l'approbation de l'entente initiale.

Le CSARS examine toutes les ententes conclues avec des organismes étrangers, tant nouvelles qu'améliorées ou renouvelées, tel que prévu au sous-alinéa 38a)(iii) de la *Loi sur le SCRS*. À cette fin, il s'emploie à déterminer si :

- les ententes du SCRS étaient conformes aux conditions énoncées dans la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle; les autorisations avaient été reçues du ministre de la Sécurité publique et du directeur du SCRS lorsque le Service avait amorcé l'échange d'information; on avait tenu compte de la réputation du pays hôte de l'organisme étranger, au chapitre des droits de la personne, entre autres des rapports publics d'organismes des droits de la personne;
- la toute dernière évaluation de l'organisme était conforme aux lignes directrices du SCRS.

Conditions à la communication d'informations par le SCRS

Le paragraphe 19(2) de la Loi sur le SCRS prévoit quatre situations où le Service peut fournir des informations obtenues dans l'exercice de ses fonctions. Selon les définitions qu'on y trouve, ces situations sont celles où l'on peut communiquer des informations :

- a) pouvant servir dans le cadre d'une enquête ou de poursuites relatives à une infraction présumée à une loi fédérale ou provinciale, et cela, aux agents de la paix compétents pour mener l'enquête, au ministre de la Sécurité publique et au procureur général de la province concernée;
- b) concernant la conduite des affaires étrangères du Canada, et cela, au ministre des Affaires étrangères;
- c) concernant la défense du Canada, et cela, au ministre de la Défense nationale;
- d) essentielles pour des raisons d'intérêt public, selon le Ministre, et cela, à un ministre ou à un fonctionnaire fédéral.

B. Ententes en vertu de l'article 17

ENTENTES AVEC DES ORGANISMES CANADIENS

Dans l'exercice de ses fonctions, le SCRS collabore souvent avec des ministères et organismes fédéraux, des gouvernements provinciaux et des organismes de maintien de l'ordre. Depuis le 11 septembre, des groupes plus nombreux s'occupent de sécurité nationale, dont des partenaires de la police et de l'extérieur du secteur public (en ce qui touche notamment les infrastructures essentielles). Cela représente un défi pour le Service, car il doit cultiver de saines relations avec tous ses partenaires, tant anciens que nouveaux, pour s'assurer que l'information est échangée efficacement et que les opérations conjointes sont menées efficacement.

COMMUNICATION D'INFORMATIONS

L'article 19 de la *Loi sur le SCRS* interdit la communication d'informations obtenues par le Service dans le cadre d'enquêtes, sauf dans des circonstances particulières. Il importe de noter que l'alinéa 19(2)d) habilite le ministre de la Sécurité publique à passer outre à toute crainte de violation de la vie privée et à autoriser le SCRS à communiquer des informations réputées être dans l'intérêt national ou public. Si de telles informations sont divulguées, le directeur du SCRS doit en faire rapport au CSARS. Par le passé, il n'y a eu que deux cas de communications visées par cet article de la *Loi*. En 2005-2006, le SCRS a affirmé au CSARS qu'il n'y en avait eu aucun.

Le Service peut aussi communiquer des informations, par écrit ou verbalement, aux organismes d'exécution de la loi ou aux entités fédérales, comme le ministère de la Défense nationale et Affaires étrangères Canada. Pour autoriser la GRC à utiliser ses informations dans des instances judiciaires, le SCRS doit le faire par écrit.

Par ses notes de communication, le SCRS autorise l'utilisation de ses informations par la GRC dans la conduite d'enquêtes criminelles. Si elle veut les utiliser devant un tribunal, la GRC doit obtenir du Service une lettre l'autorisant à le faire.

Le tableau qui suit est une compilation des communications d'informations par le Service en vertu de l'article 19, par direction.

Tableau 2
Communications d'informations par le SCRS en vertu de l'article 19 de la *Loi sur le SCRS*

Direction	Organismes d'exécution de la loi (a)	Affaires étrangères Canada (b)	Ministère de la Défense nationale (c)	Intérêt public (d)
Antiterrorisme	293	0	4	0
Contre-espionnage	19	0	0	0
Lutte contre la prolifération	23	1 340	2 353	0
Total	335	1 340	2 357	0

(a) Communication en vertu de l'alinéa 19(2)a)
(b) Communication en vertu de l'alinéa 19(2)b)
(c) Communication en vertu de l'alinéa 19(2)c)
(d) Communication en vertu de l'alinéa 19(2)d)

CERTIFICAT DE L'INSPECTEUR GÉNÉRAL (2005)

Le poste d'inspecteur général (IG) a été créé en 1984 en vertu de la *Loi sur le SCRS*. Son titulaire joue, pour le ministre de la Sécurité publique, le rôle de « vigile » scrutant les opérations du Service et fournissant l'assurance que celui-ci respecte la *Loi sur le SCRS*, les instructions ministérielles et la politique opérationnelle.

Chaque année, l'inspecteur général fait parvenir au Ministre un certificat exposant dans quelle mesure il est satisfait du rapport annuel du directeur du SCRS. Il l'informe de tout cas où le SCRS aurait négligé de se conformer à la *Loi* ou aux instructions ministérielles et où il aurait exercé ses pouvoirs de façon abusive ou inutile.

Dans le dernier certificat, l'IG a mentionné que le directeur du SCRS avait signalé trois incidents de non-respect de la politique opérationnelle en 2004-2005. Après les avoir examinés, elle a constaté que des mesures appropriées avaient été prises dans chaque cas. L'IG a aussi relevé deux autres cas de non-respect. Cependant, elle a affirmé que la seule action corrective qui s'imposait était que l'on porte davantage d'attention au respect des échéanciers établis.

L'IG s'est aussi dite étonnée de plusieurs affirmations erronées, relevées dans le rapport du directeur. Deux d'entre elles avaient trait à des erreurs statistiques, mais d'autres concernaient des questions plus fondamentales, à son avis. Comme on peut le lire dans le certificat, le Service a admis les affirmations erronées et informé l'IG que des mesures correctives seraient prises.

L'IG a mentionné en conclusion que le Service avait apporté plus promptement, au personnel de son bureau, l'aide demandée pour son travail. « Les préoccupations que j'ai exprimées précédemment, a-t-elle ajouté, n'ont aucunement pour but de dépeindre les efforts acharnés et consciencieux déployés par le SCRS et ses employés pour servir le Canada et lutter contre les menaces envers la sécurité de l'État. »

Pour plus d'information, prière de vous reporter à la page d'accueil du Bureau de l'inspecteur général, sur le site Web de Sécurité publique (www.pspc-spcc.gc.ca).

AGISSEMENTS ILLICITES DE LA PART DU SCRS

En vertu du paragraphe 20(2) de la *Loi sur le SCRS*, le directeur du Service doit présenter un rapport au Ministre s'il estime qu'un employé du SCRS peut avoir commis un acte illicite dans l'exercice de ses fonctions. Le cas échéant, le Ministre doit alors transmettre ce rapport au procureur général du Canada et au Comité, accompagné de ses observations.

En 2005-2006, il n'y a eu aucune activité requérant un tel rapport.

A. Exigences en matière de rapports

RAPPORT ANNUEL DU DIRECTEUR DU SCRS (2004-2005)

Chaque année, le directeur du SCRS doit présenter au ministre de la Sécurité publique un rapport très secret, décrivant en détail les priorités et les activités opérationnelles du Service. Selon la *Loi sur le SCRS*, l'inspecteur général du SCRS est tenu d'examiner ce rapport et de faire parvenir au Ministère un certificat attestant dans quelle mesure il est satisfait de son contenu. Enfin, le Ministère transmet copie des deux documents au CSARS afin qu'il les examine, tel que prescrit à l'alinéa 38a) de la *Loi sur le SCRS*.

Dans son rapport de 2004-2005, le directeur affirme qu'en appuyant la toute première priorité du Service, soit la sécurité du public, le SCRS s'emploie à empêcher qu'un attentat terroriste soit perpétré ou préparé au Canada. Le directeur a mentionné que cela a une incidence sur les ressources de l'organisme et il expose les stratégies employées pour relever ce défi.

Le directeur attire en outre l'attention sur une nouvelle dimension de la menace représentée par l'extrémisme islamique. La menace d'Al-Qaïda demeure très grave à l'étranger, mais un attentat terroriste en sol canadien est maintenant considéré comme probable. Pour la première fois, le SCRS a aussi averti de la menace relativement nouvelle que représentaient les terroristes d'origine intérieure.

Dans son rapport, le directeur affirme en outre que le Service continue d'enquêter sur les tentatives de pays étrangers pour espionner les communautés d'expatriés au Canada et pour s'immiscer dans leurs affaires.

Dans son rapport, le directeur souligne les efforts du SCRS pour resserrer la coopération avec ses partenaires canadiens. Il y fait en outre état des excellentes relations du Service avec ses principaux partenaires étrangers et du fait que celui-ci a prêté main-forte à des services de renseignement étrangers d'États fraîchement démocratiques, en donnant une formation sur les principes et méthodes de la collecte de renseignements.

Le rapport contient des détails sur les programmes du Service relatifs aux sources humaines et au filtrage de sécurité et une description de sa conformité aux instructions ministérielles et aux exigences nationales émanant du ministre de la Sécurité publique.

Le lecteur est prié de noter que le SCRS affiche sur son site Web (www.csis-scs.gc.ca) des rapports non classifiés.

Section 2

Mécanismes additionnels du SCRS

- rappelle à ses employés que tous leurs documents peuvent être assujettis à la *Loi sur l'accès à l'information*, à la *Loi sur la protection des renseignements personnels* et à la politique opérationnelle et qu'ils ne peuvent être éliminés que suivant les politiques du Service à cet égard;
- instaure une politique prescrivant de conserver un rapport d'évaluation de la haute direction sur la fiabilité et la pertinence de déclarations verbales et écrites avant de décider de la manière de clore une enquête de la Sécurité interne;
- affiche, dans les bureaux des Services de Santé et sur tout site Web concernant le Programme d'aide aux employés (PAE) du SCRS, un avis portant que les communications avec une personne autre qu'un conseiller, au sens de la politique du PAE, ne sont assujetties à aucun code de confidentialité. Le personnel affecté au PAE doit informer les participants qui demandent de l'aide en vertu de ce programme que seules les communications avec un conseiller sont assujetties à un tel code;
- modifie sa politique concernant le PAE de manière à prescrire que des mesures raisonnables soient prises pour assurer que tout consentement requis d'un employé soit donné librement et volontairement, et qu'un document décrivant ces mesures soit conservé au dossier de l'employé;
- modifie les politiques du SCRS relatives aux ressources humaines de manière à obliger les surveillants et les autres membres du personnel à informer leurs gestionnaires ou le gestionnaire de l'employé en question s'ils ont des motifs de croire que celui-ci a besoin d'une aide médicale.

Présumée réactive inapprouvée à la maladie d'un plaignant

RAPPORT N° 4

Le Comité a fait rapport d'une décision concernant une plainte portée en vertu de l'article 41 de la *Loi sur le SCRS*. Selon cet article, toute personne peut porter plainte contre « des activités du Service ».

Le plaignant, ancien employé du SCRS, a prétendu que celui-ci avait :

- forcé le plaignant à demeurer au travail et à avouer des actes qu'il n'avait pas posés;
- violé le code de confidentialité du Programme d'aide aux employés (PAE);
- négligé de porter assistance au plaignant au moment où il avait besoin d'une aide médicale.

Le CSARS a constaté que les effets du stress et de l'épuisement, combinés à l'incertitude de l'issue du processus disciplinaire, auraient incité le plaignant à demeurer au travail et à faire des déclarations compromettantes dans des circonstances qui les avaient rendues non fiables. Le Comité soutient en outre que le SCRS a omis tant d'évaluer la fiabilité de l'aveu du plaignant que de lui fournir l'occasion de répondre à une nouvelle infraction présumée, avant de le licencier.

Le CSARS a constaté qu'une personne raisonnable prendrait pour une « consultation » à l'endroit du plaignant les actions du chef des Services de santé, qui était chargé de la politique du PAE. En conséquence, il a constaté que le code de confidentialité avait été violé du fait que le chef des Services de santé avait amené un enquêteur à prendre une déclaration du plaignant.

Le CSARS a recommandé que le Service :

- note au dossier personnel du plaignant que certaines déclarations de celui-ci ont été faites dans des circonstances telles que ces déclarations doivent être considérées comme non fiables;
- veille à se conformer à la politique « Écarts de conduite et mesures disciplinaires » avant d'imposer de telles mesures à un employé;
- instaure une politique prescrivant de verser, dans tous les dossiers d'enquête de la Sécurité interne, toute information pertinente de nature à influencer la fiabilité de déclarations (p. ex., la capacité de l'intéressé à faire une déclaration libre et volontaire);

RAPPORT N° 3

Le CSARS a fait rapport d'une décision concernant une plainte dont la Commission canadienne des droits de la personne l'avait saisi en vertu de l'article 45 de la Loi canadienne sur les droits de la personne (LCDP).

Le plaignant, ancien employé du SCRS, souffrait d'une maladie répondant à la définition d'invalidité énoncée dans la LCDP. Il a été allégué qu'au lieu de prendre des moyens permettant à l'employé d'exercer ses fonctions, le Service avait profité de cette invalidité pour en obtenir des déclarations et le licenciement. Il a aussi été allégué que le SCRS avait refusé au plaignant sa demande de prorogation du délai de 25 jours pour en appeler de son renvoi ou présenter un grief.

Le Comité a constaté que, lorsqu'il travaillait pour le SCRS, le plaignant souffrait d'une invalidité au sens de l'article 7 de la LCDP. Il a aussi conclu à l'existence de preuves que le Service savait ou aurait dû savoir que le plaignant souffrait d'une invalidité.

Le CSARS a établi que le SCRS avait traité le plaignant de façon défavorable en invoquant des déclarations antérieures de celui-ci comme motifs de son licenciement. En conséquence, le CSARS a convenu que le plaignant avait été l'objet de discrimination présumée pour un motif illégitime, selon la LCDP. Il a soutenu que le SCRS aurait dû répondre aux besoins du plaignant en demandant un examen de son état de santé et qu'il aurait dû lui donner la chance de répondre aux allégations avant de le licencier.

Le CSARS a recommandé que :

- les politiques du SCRS relatives aux ressources humaines et portant sur l'examen de l'état de santé soient modifiées de manière que les surveillants et les autres membres du personnel soient tenus d'informer leurs gestionnaires ou le gestionnaire de l'employé visé s'ils ont des motifs de croire que celui-ci a besoin d'une aide médicale;
- le Service permette au plaignant de présenter un grief;
- si la Commission canadienne des droits de la personne décide d'enquêter sur les allégations du plaignant, elle ne rende publique aucune information qui, selon le rapport du CSARS, suscite des craintes en matière de sécurité nationale.

Le CSARS a aussi constaté que cette affaire n'était pas équitable du point de vue procédural, de la part du ministère employeur, le plaignant n'ayant pu répondre aux allégations avant qu'il soit décidé de lui refuser une habilitation de sécurité. Le ministère employeur n'avait pas informé celui-ci des raisons du refus, ni des préoccupations exprimées par le SCRS en matière de sécurité.

Le CSARS a recommandé que :

- l'habilitation de sécurité demandée soit octroyée au plaignant;
- le SCRS vérifie ou corrobore les renseignements d'habilitation sécuritaire fournis par un demandeur ou par des sources, s'il peut le faire facilement;
- le ministère ou organisme employeur clarifie sa procédure de façon que, dans ces circonstances, l'intéressé obtienne des renseignements sur toute constatation défavorable du SCRS. Cela doit se faire de manière à respecter la sécurité nationale mais à permettre à l'intéressé de connaître les raisons du refus d'une habilitation de sécurité;
- le SCRS et le ministère ou organisme employeur tiennent tous deux compte d'observations récentes du commissaire à la protection de la vie privée, soit que, du fait que les organismes veillant à l'exécution de la loi et à la sécurité nationale accueillent plus de renseignements de sources plus nombreuses, on risque d'avantage qu'une information d'exactitude douteuse puisse infléchir des décisions ou soit prise hors contexte;
- le ministre responsable du ministère ou organisme employeur écrive à l'ancien député fédéral du plaignant pour lui faire savoir que, contrairement à une information antérieure, il n'y avait aucune preuve que la personnalité du plaignant ou ses relations antérieures affecteraient l'admissibilité de celui-ci à une habilitation de sécurité de quelque niveau que ce soit;
- le ministère ou organisme employeur prenne des mesures pour assurer la qualité et l'exactitude de l'information qui est transcrite à partir de fiches de renseignements personnels remplies à la main.

Voir Commissariat à la protection de la vie privée, *Rapport annuel au Parlement 2004 : rapport sur la Loi sur la protection des renseignements personnels et les documents électroniques*, page 15.

Tout d'abord, le CSARS a conclu que l'avis de refus contenait un exposé injuste et inexact, préjudiciable à l'intéressé, de l'information dont disposait le SCRS lorsqu'il a ouvert l'enquête d'habilitation de sécurité. Ensuite, il a conclu que l'avis reposait sur une enquête dans le milieu, menée par un enquêteur inexpérimenté du SCRS, qui avait tiré des conclusions non fondées.

Le CSARS n'a trouvé aucun élément de preuve fiable étayant la conclusion que le plaignant pouvait participer à des activités constituant une menace envers la sécurité du Canada ou révéler des renseignements classifiés sans autorisation.

Le CSARS a recommandé que :

- l'administrateur général du ministère ou de l'organisme fédéral compétent octroie au plaignant la cote de sécurité demandée;
- le Service arrête une procédure visant à assurer que des notes exactes soient prises, ou un enregistrement fait, aux entrevues de filtrage de sécurité. Ces notes ou enregistrement devraient être conservés pendant cinq ans après une entrevue, ou même plus longtemps si l'intéressé conteste les résultats de l'enquête de sécurité.

En réponse à cette dernière recommandation, en décembre 2005, le SCRS a informé le CSARS qu'il avait revu ses pratiques concernant la consignation de notes et l'enregistrement des entrevues avec le consentement des intéressés. Les enquêteurs sont maintenant tenus d'offrir d'enregistrer l'entrevue d'un sujet si celle-ci est faite pour le filtrage de sécurité d'un employé de l'État. Le Service maintiendra son obligation de rédiger un compte rendu complet et exact des échanges, que le sujet consente ou non à l'enregistrement de l'entrevue.

Refus d'une habilitation de sécurité

RAPPORT N° 2

Le CSARS a fait rapport d'une deuxième décision, également en vertu de l'article 42 de la *Loi sur le SCRS*, au sujet du refus d'une habilitation de sécurité.

Le CSARS a constaté que la décision de refuser l'habilitation de sécurité était fondée sur une information incomplète et parfois inexacte. Certaines informations corroborées, favorables au plaignant, ne figuraient pas dans l'avis de refus. De plus, le CSARS a constaté que les craintes signalées par le ministère employeur, au sujet de la loyauté et de la fiabilité du plaignant, n'étaient pas étayées par les éléments de preuve recueillis à l'audience de la plainte.

Nouvelle procédure

Au cours de 2005-2006, le CSARS a élaboré de nouvelles pratiques, en consultation avec le SCRS, afin de simplifier le processus d'enquête sur les plaintes et d'assurer l'équité de la procédure.

Premièrement, des changements ont été apportés à la manière dont le Service communique les documents au CSARS. Il importe de noter que l'accès de celui-ci à l'information en ce domaine n'est restreint que par le paragraphe 39(3) de la *Loi sur le SCRS*, selon lequel le Service peut refuser au CSARS les documents confidentiels du Cabinet. Une nouvelle procédure a été adoptée, fondée sur le principe de la production continue qui est prévu au paragraphe 226(1) des *Règles de la Cour fédérale* et au paragraphe 6(5) des *Règles de procédure du Tribunal canadien des droits de la personne*. Ce principe permet au SCRS de notifier le Comité promptement s'il constate que des documents concernant une plainte n'ont jamais été mis à la disposition du CSARS.

Une autre innovation est la « conférence préparatoire à l'audience ». Cette conférence, qui a été instaurée en janvier 2006, est dirigée par un président, membre du CSARS, en présence de toutes les parties. Elle vise à résoudre les questions de procédure préliminaires (p. ex., les allégations devant faire l'objet d'une enquête, l'identité et le nombre des témoins à citer). Dans la mesure où l'on n'y aborde aucune question liée à la sécurité nationale, la conférence peut se tenir au téléphone, après quoi une transcription est remise aux parties.

Le 31 mars 2006, le CSARS avait tenu quatre conférences préparatoires à audience.

Décisions du CSARS sur les plaintes en 2005-2006

Voici les résumés des décisions que le Comité a rendues au cours de la période à l'étude en réponse aux plaintes qui lui avaient été présentées.

Rapport de l'enquête sur la plainte portée dans l'affaire Bhupinder Liddar

RAPPORT N° 1

Une plainte a été présentée au CSARS en vertu de l'article 42 de la *Loi sur le SCRS* après que le plaignant, M. Bhupinder Liddar, se soit vu refuser une habilitation de sécurité suivant une recommandation (dire « avis de refus ») du Service.

Après étude de la plainte, le Comité a constaté qu'il n'y avait pas de fondement raisonnable à cette recommandation et que celle-ci était inexacte et trompeuse pour plusieurs raisons.

Détermination de la compétence à examiner une plainte en vertu de l'article 42

En ce qui a trait aux décisions d'administrateurs généraux fédéraux de refuser une habilitation de sécurité, selon l'article 42 de la Loi sur le SCRS, le Comité de surveillance enquête sur les plaintes présentées par :

- 1. les personnes qui ne sont pas embauchées par le gouvernement fédéral à cause du refus d'une habilitation de sécurité;
- 2. les fonctionnaires fédéraux qui sont renvoyés, rétrogradés ou mutés ou qui se voient refuser une promotion ou une mutation pour la même raison;
- 3. les personnes qui se voient refuser un contrat de fourniture de biens ou de services au gouvernement, toujours pour le même motif.

Une plainte ressortissant à l'article 42 de la Loi doit être présentée dans les 30 jours du refus d'une habilitation de sécurité. Le CSARS peut prolonger cette période si on lui fait part de raisons valables.

Le tableau 1 montre l'état de toutes les plaintes qui ont été présentées au CSARS au cours des trois derniers exercices, y compris celles qui lui ont été adressées à tort, qui ont été déclarées hors de sa compétence ou qui ont fait l'objet d'une enquête et d'un règlement sans audience (examen administratif).

Tableau 1
Règlement des plaintes*

	2003-2004	2004-2005	2005-2006
Reportées de l'exercice précédent	17	16	18
Nouvelles	30	30	45
Total	47	46	63
Réglées	31	28	39
Reportées à l'exercice suivant	16	18	24
Rapports présentés	1	3	4

* Fait état de l'ensemble des plaintes que le Comité a reçues et dont l'étude n'a pas forcément débouché dans chaque cas sur une enquête. Certaines plaintes ont été renvoyées à un autre organisme gouvernemental ou déclarées hors de la compétence du CSARS. D'autres ont été retirées par leur auteur.

Selon la *Loi sur le SCRS*, les personnes qui se voient refuser une habilitation de sécurité doivent en être avisées par l'administrateur général de leur organisme. Elles ont le droit de porter plainte au CSARS qui, s'il y a lieu, fait enquête et présente ses constatations et recommandations au Ministre, au directeur du SCRS et à l'administrateur général. Le Comité remet aussi au plaignant un rapport exposant ses constatations et tenant compte de l'obligation de protéger les renseignements classifiés.

Si la Commission canadienne des droits de la personne reçoit d'un ministre fédéral un avis écrit concernant une plainte qui a trait à la sécurité du Canada, elle peut en saisir le CSARS. Sur réception d'un tel renvoi, le Comité fait enquête et présente ses constatations à la Commission, à l'intimé et au plaignant. Il a aussi le pouvoir d'enquêter sur les affaires qui lui sont renvoyées en vertu de la *Loi sur la citoyenneté*.

Détermination de la compétence à examiner une plainte en vertu de l'article 41

En vertu de l'article 41 de la *Loi sur le SCRS*, le Comité enquête sur les plaintes que « toute personne » peut porter contre « des activités du Service ». Pour qu'il fasse enquête, deux conditions doivent être remplies :

1. le plaignant doit d'abord avoir présenté sa plainte par écrit au directeur du SCRS sans recevoir de réponse dans un délai raisonnable (environ 30 jours) ou, s'il en a reçu une, sans que cette réponse le satisfasse;

2. le Comité doit être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet ni entachée de mauvaise foi.

Conformément au paragraphe 41(2) de la *Loi*, le CSARS ne peut enquêter sur une plainte qui peut être réglée autrement, par une procédure de griefs établie en vertu de la *Loi sur le SCRS* ou de la *Loi sur les relations de travail dans la fonction publique* (autrefois appelée *Loi sur les relations de travail dans la Fonction publique*).

Les types de plaintes sur lesquelles le CSARS enquête sont décrits dans la *Loi sur le SCRS* et prennent diverses formes. En vertu de l'article 41 de la *Loi*, le CSARS peut faire enquête sur n'importe quelles « activités du Service ». Selon l'article 42, il peut instruire les plaintes concernant le refus d'habilitations de sécurité à des fonctionnaires et à des fournisseurs de l'État (voir « *Détermination de la compétence à examiner une plainte en vertu des articles 41 et 42* »). L'article 42 n'habilite pas le Comité à reconnaître sa compétence à instruire les plaintes concernant les contrôles d'antécédents ou les vérifications de fiabilité, à caractère moins intrusif, qui sont généralement menés simplement pour déterminer la loyauté ou l'aptitude d'un fonctionnaire fédéral éventuel. Pour l'étude de ces plaintes, on suit la procédure de grief prévue par l'organisme intéressé.

Types de plaintes

Le Comité peut faire enquête sur quatre types d'affaires :

- les plaintes de particuliers « contre des activités du Service » (article 41);
- celles concernant le refus d'habilitations de sécurité à des fonctionnaires et à des fournisseurs de l'État (article 42);
- les allégations dont la Commission canadienne des droits de la personne saisit le CSARS;
- les rapports du Ministre à l'égard de la *Loi sur la citoyenneté*.

Un plaignant a le droit d'être représenté par un avocat et de formuler des observations à l'audience. Une audience préliminaire peut être tenue pour arrêter une procédure, de concert avec le plaignant ou son avocat ou avec les deux. L'avocat principal du Comité fournit des avis juridiques concernant la procédure et les questions de fond et il contre-interroge aussi les témoins du Service si ceux-ci doivent être entendus en l'absence du plaignant, pour des raisons liées à la sécurité nationale.

À la suite d'une audience, le Comité rédige un rapport énonçant les recommandations qu'il juge indiquées. Ce rapport est envoyé à la fois au ministre de la Sécurité publique et au directeur du SCRS. Tout renseignement ayant des incidences sur le plan de la sécurité nationale est supprimé de la version du rapport qui est transmise au plaignant. Les résumés de ces rapports, expurgés de manière à protéger la sécurité nationale et la vie privée des intéressés, figurent également dans le rapport annuel du CSARS au Parlement.

L'exploitation des sources humaines a été efficace, mais le CSARS a constaté un manque de coordination dans l'exploitation conjointe d'une source par deux régions. Il a aussi constaté qu'une source avait été dirigée contre des cibles au sein d'une institution névralgique avant que l'autorisation appropriée n'ait été obtenue, quoique celle-ci n'ait alors pas tardé à venir.

Le CSARS s'est interrogé sur l'emploi d'une certaine technique d'interception par le Service et il a recommandé que celui-ci obtienne une opinion juridique à jour sur l'emploi de cette technique particulière.

L'examen des mesures de sécurité interne, y compris les manquements et infractions, est un volet habituel de toute étude régionale. Le CSARS a constaté que les problèmes de sécurité interne étaient traités de façon irréprochable par la région, sauf par un bureau de district où des manquements possibles n'étaient pas documentés. Même si on lui a fourni l'assurance que d'autres mécanismes internes auraient empêché tout manquement, le CSARS a recommandé que tous les bureaux régionaux se conforment strictement à la politique opérationnelle en place, quels que soient l'endroit où ils sont situés ainsi que leur taille ou leur effectif.

B. Enquêtes sur les plaintes

Procédure d'enquête du CSARS sur les plaintes

Outre sa fonction de surveillance, le Comité a charge d'enquêter sur les plaintes du public au sujet du SCRS. La première étape de presque tout dossier de plainte est une demande de renseignements au CSARS. Celle-ci peut être faite par écrit, en personne ou par téléphone. Le personnel du Comité y répond sur-le-champ, indiquant généralement au plaignant éventuel les exigences de la *Loi sur le SCRS* pour que son affaire soit considérée à titre de plainte officielle. Lorsqu'il reçoit une plainte par écrit, le CSARS fait un examen initial.

Si la plainte ne répond pas à certaines exigences de la loi, le CSARS ne reconnaît pas sa compétence et n'enquête pas. S'il la reconnaît, il examine la plainte lors d'une audience quasi judiciaire que préside un ou plusieurs de ses membres, secondés par le personnel. Dans ses enquêtes sur les plaintes, le CSARS a tous les pouvoirs d'une cour supérieure et il a accès à toute information que le SCRS peut avoir en sa possession, à l'exception des documents confidentiels du Cabinet.

Contexte

Le CSARS examine souvent les activités du SCRS dans une région particulière du Canada. Ces études régionales permettent de savoir de quelle manière les enquêtes autorisées par l'Administration centrale du SCRS sont menées en région, et elles aident le CSARS à connaître plus à fond les activités, les priorités et les difficultés des régions.

Cette étude régionale arrivait à point nommé, car elle a permis au CSARS d'examiner la première enquête, autorisée par un mandat, sur une menace nouvelle pour le Canada : les convertis d'origine canadienne à l'extrémisme islamique.

Méthode

Au sujet de l'enquête autorisée par un mandat, le CSARS a évalué dans quelle mesure le Service avait respecté la *Loi sur le SCRS*, les instructions ministérielles et la politique opérationnelle pertinente, en examinant :

- la demande et l'exercice, par le Service, des pouvoirs conférés par mandat, et les opérations spéciales;
- le processus du SCRS pour l'autorisation des enquêtes et la conduite de celles-ci contre les cibles;
- le recrutement et l'essai de sources humaines par le Service et l'attribution de missions à celles-ci;
- la coopération, la liaison et les échanges d'information du SCRS avec ses partenaires canadiens;
- les mesures et la procédure de sécurité interne du Service.

Cet examen a porté sur la période du 1^{er} janvier 2002 au 31 décembre 2004.

Constatations

Le CSARS est d'accord avec l'évaluation du Service selon laquelle les convertis d'origine intérieure à l'extrémisme islamique représentent une menace grave pour la sécurité nationale. Les enquêtes du SCRS lui ont permis d'identifier plusieurs individus qui participaient à la planification d'actes terroristes ou prenaient part à des activités de collecte de fonds, de recrutement et d'entraînement. Le CSARS a constaté que la description des activités liées à la menace par la région, dans les demandes de mandats, traduisait fidèlement l'information que le Service avait en main. De plus, l'étendue des pouvoirs demandés par la voie de mandats et exercés ultérieurement par le Service allait de pair avec la menace et était conforme à la *Loi sur le SCRS*, à toutes les conditions énoncées par la Cour fédérale et à la politique opérationnelle même du Service.

Certains groupes ont exprimé des craintes au sujet de l'impact que ce projet de loi aurait pu avoir sur le droit au respect de la vie privée au Canada. Le CSARS estime qu'un cadre légal actualisé pourrait toutefois apaiser ces craintes, ce qui mettrait le Canada sur un pied d'égalité avec d'autres alliés proches. Il est bon de noter que, selon un sondage d'opinion mené en 2006, 49 p. 100 des Canadiens sont d'avis que les organismes d'exécution de la loi et de sécurité devraient avoir des pouvoirs accrus pour assurer la sécurité, même si cela signifiait que les Canadiens doivent renoncer à certaines garanties à leur vie privée¹.

Méthode

Le CSARS a examiné deux demandes de mandat approuvées par la Cour fédérale en 2004, l'une concernant une enquête de contre-espionnage et l'autre, une enquête antiterroriste. Il a étudié les documents, versions papier et électronique, ayant trait à chacune des demandes, ainsi que l'exercice des pouvoirs prévus dans les mandats contre les sources autorisées.

Constatations

Le CSARS a constaté que le Service avait respecté la *Loi sur le SCRS* et toutes les politiques opérationnelles pertinentes dans sa demande de mandats et dans l'exercice des pouvoirs conférés par ceux-ci pour appuyer l'enquête de contre-espionnage.

Le CSARS a constaté que, contrairement à la politique opérationnelle, le SCRS avait continué de recueillir des renseignements sur une cible antiterroriste pendant une brève période après avoir clos son enquête. Le SCRS a toutefois confirmé qu'il n'avait pas traité cette information et qu'il l'avait par la suite supprimée. De plus, le CSARS ne savait guère pourquoi le SCRS croyait avoir besoin de se faire octroyer des pouvoirs par la voie de mandats pour enquêter sur une autre cible antiterroriste.

Le CSARS a aussi relevé certains retards administratifs du SCRS à présenter les documents relatifs à l'exercice des pouvoirs prévus dans les mandats contre certaines cibles antiterroristes. Il a en outre constaté que plusieurs autres dossiers d'exécution de mandat ne contenaient pas tous les documents exigés par la politique opérationnelle.

Le Comité a convenu avec le SCRS que différentes situations peuvent requérir divers types de documents et que ces exigences peuvent changer au fil du temps. Pour les besoins de la reddition de comptes et de l'efficacité, cependant, le CSARS a recommandé que le SCRS examine et retouche la politique en question sur les mandats afin qu'elle reflète les pratiques exemplaires actuelles. Conformément à cette recommandation, le SCRS a entrepris de revoir sa politique à cet égard.

¹ *Security Monitor (Wave 6)*, Ekos Public Opinion Research, juin 2006, page 16.

Examen des techniques de surveillance électronique et de collecte d'information du SCRS

Rapport n° 2005-07

Contexte

Lors de la création du SCRS en 1984, le Canada comptait moins de dix grandes compagnies de téléphone en exploitation et il faudra une décennie pour que l'Internet devienne un norm familial. Depuis, les services de télécommunication ont connu une croissance exponentielle, tout comme les activités des Canadiens en ligne.

L'évolution rapide des technologies a entraîné des changements radicaux dans les types de techniques qui peuvent servir à la surveillance électronique. Les progrès des communications à large bande et sans fil défont de plus en plus la capacité du SCRS et des services policiers à se procurer en toute légalité les renseignements requis pour assurer la sécurité du public. Actuellement, les fournisseurs canadiens de services de téléphone et d'Internet ne sont pas tenus de doter leurs réseaux d'une capacité d'interception ou de maintenir une telle capacité. Aussi, quand une nouvelle technologie voit le jour, le SCRS et la police doivent-ils souvent mener des recherches en vue de concevoir des moyens uniques et coûteux d'avoir accès légalement à ces réseaux.

Le rythme des changements technologiques et la rapidité avec laquelle terroristes et services de renseignement étrangers adoptent ces innovations font que les organismes canadiens d'exécution de la loi et de sécurité doivent demeurer à la fine pointe du progrès. Le CSARS doit leur emboîter le pas pour continuer à s'acquitter de sa fonction d'examen.

Actuellement, le paragraphe 21(3) de la *Loi sur le SCRS* habilite le Service, moyennant autorisation d'un juge de la Cour fédérale, « à intercepter des communications ou à acquérir des informations, documents ou objets ». Le Canada est toutefois l'un des rares pays du G8 à ne pas avoir de loi obligeant les entreprises à se doter d'une capacité d'interception. La *Loi sur la modernisation des techniques d'enquête*, qui avait été proposée, aurait comblé cette lacune.

Le gouvernement du Canada a déposé la *Loi sur la modernisation des techniques d'enquête* en novembre 2005, mais celle-ci n'avait été adoptée qu'en première lecture lors de la dissolution du Parlement, avant l'élection fédérale. Une loi semblable existe toutefois depuis plusieurs années dans d'autres pays, dont les États-Unis, le Royaume-Uni et l'Australie. Vous trouverez de plus amples renseignements sur le site Web de Sécurité publique (www.psepc-sppcc.gc.ca).

lettre et qu'il devrait trouver un moyen de la corroborer lui-même avant d'en déterminer la fiabilité ». Le SCRS a en outre reconnu que, dans la plupart des cas, « il ne sait pas si une information découle d'une violation des droits de la personne, [mais] s'il a des soupçons, il doit faire la part entre cela et la nécessité d'obtenir l'information en vue de protéger les Canadiens et les intérêts canadiens ».

Le SCRS a mentionné que les employés sont censés scruter de près l'information fournie à des organismes, ou reçue d'eux, dans les pays au bilan douteux en matière de respect des droits de la personne, et qu'ils sont invités à faire preuve de diligence raisonnable lorsqu'ils évaluent l'information qu'ils en obtiennent. Le Service a affirmé que l'on tient compte des questions liées aux droits de la personne dans le processus des échanges, mais qu'aucune politique opérationnelle particulière n'oblige actuellement à le faire.

Le CSARS reconnaît que, si le SCRS doit protéger la sécurité du Canada, il lui faut entretenir des relations et échanger de l'information avec des organismes du monde entier, dont certains ont un bilan douteux au titre du respect des droits de la personne. Néanmoins, le CSARS est d'avis que le cadre stratégique du SCRS devrait refléter les défis que celui-ci doit relever en traitant avec des pays soupçonnés de violer ces droits.

Le CSARS a recommandé que le SCRS modifie sa politique sur la communication d'information à des organismes étrangers de manière à prévoir la prise en compte de la réputation des pays intéressés, au chapitre des droits de la personne, et des violations possibles de la part de leurs services de sécurité ou de renseignement.

Dans le cadre de son étude, le CSARS a aussi relevé les mentions de conversations téléphoniques protégées entre un agent de liaison-sécurité (ALS) en poste à l'étranger et l'Administration centrale du SCRS. Lorsque le CSARS s'est informé du contenu de ces conversations, le Service lui a répondu qu'il n'y avait pas de comptes rendus de ces discussions verbales.

En conséquence, le CSARS a recommandé que l'Administration centrale du SCRS tienne un compte rendu des conversations téléphoniques protégées avec les ALS, en particulier de celles contenant des renseignements opérationnels, et que ce compte rendu figure dans ses rapports.

Le CSARS a aussi appris que le SCRS ne discute généralement en détail, avec les organismes étrangers, des paramètres et conditions des ententes, qu'après avoir conclu ces ententes avec les intéressés. Le CSARS estime que ces questions devraient être abordées plus tôt dans le processus de conclusion des ententes.

Le CSARS a recommandé que le SCRS revoise sa procédure de manière à communiquer aux organismes étrangers les paramètres et les méthodes d'échange, de même que ses attentes, avant de conclure de nouvelles ententes avec eux.

Pour chaque organisme étranger, le CSARS a examiné :

- les motifs justifiant la conclusion de l'entente et, le cas échéant, son élargissement;
- la relation entre le SCRS et l'organisme;
- la nature de l'information partagée;
- les conditions ou restrictions spéciales dont était assortie la collecte ou l'utilisation de cette information;
- une évaluation des renseignements divulgués à l'organisme étranger et reçus de lui.

L'examen a porté sur la période du 1^{er} janvier 2002 au 31 décembre 2004. Certaines informations ont aussi été demandées, débordant cette période.

Constatations

Dans l'ensemble, le CSARS a constaté que les échanges d'information du SCRS avec ces organismes entraient dans le champ des ententes conclues respectivement avec chacun d'eux, et que le Service avait respecté la *Loi sur le SCRS*, les instructions ministérielles et la politique opérationnelle.

Le CSARS a toutefois relevé certaines craintes. Premièrement, il a constaté que, même si la communication de certains renseignements à un organisme étranger par le SCRS était à l'abri de tout reproche, elle pouvait avoir contribué à la décision de cet organisme de détenir un citoyen canadien (qui était aussi une cible du Service) à son arrivée dans ce pays étranger.

Le CSARS est convaincu que le même
stratégie du SCRS devait
réfléter les défis que celui-ci doit
relever en traitant avec des pays
suspenses de violer les droits de
la personne.

Deuxièmement, le CSARS a craint que l'information reçue d'un organisme étranger par le SCRS, et utilisée par celui-ci, n'ait été obtenue sous la contrainte, même si le Service avait mené les échanges en question de façon irréprochable. Le CSARS a aussi noté que les questions posées par le SCRS à cet organisme par l'entremise d'un tiers pouvaient avoir servi à interroger un citoyen canadien d'une manière qui violait ses droits humains. Selon l'évaluation du Service, ces deux individus étaient une menace et il s'est prému des autorisations nécessaires en vue d'ouvrir des enquêtes. Le CSARS n'est toutefois pas en mesure d'examiner si les autres organismes canadiens ou étrangers, qui enquêtaient aussi sur ces individus, peuvent avoir contribué à la détention et/ou à l'interrogatoire de ceux-ci.

Au sujet de l'information qui pouvait avoir été obtenue par le biais de violations de droits humains, le CSARS a demandé au SCRS s'il l'avait traitée différemment de celle obtenue par d'autres moyens. Il lui a répondu qu'il ne prenait « aucune information au pied de la

Le Service a mis fin à son enquête au cours de la période étudiée. Le Comité a noté qu'il avait mené une enquête approfondie sur toutes les activités présumées d'espionnage et d'ingérence étrangère et il a constaté qu'elles n'étaient pas appuyées par des preuves corroborantes ou qu'elles étaient des incidents isolés. De plus, le Service a assuré au CSARS qu'il était prêt à faire face, de façon ponctuelle, à toute menace future représentée par le service de renseignement étranger en question.

D'après l'information dont il disposait pour son étude, le CSARS a convenu de l'évaluation du SCRS, soit que ce service de renseignement étranger n'était plus une menace pour la sécurité du Canada.

Cette étude n'a donné lieu à aucune recommandation.

Étude n° 2005-05

Nota :

le CSARS travaille actuellement à l'étude n° 2005-05 qui n'était toutefois pas finalisée au moment de mettre sous presse. Un résumé de cette étude figurera dans le rapport annuel de 2006-2007 du Comité.

Examen des ententes conclues avec des pays soupçonnés de violer les droits de la personne

Rapport n° 2005-06

Contexte

La *Loi sur le SCRS* habilite le Service à conclure des ententes visant à échanger de l'information concernant les menaces à la sécurité du Canada avec des services de renseignement étrangers. Dans le cas de pays ayant un engagement douteux envers les droits humains, la conclusion d'ententes avec eux n'est envisagée, selon les instructions ministérielles, que si la sécurité du Canada le requiert. Une fois qu'il a conclu une entente avec un organisme étranger, le SCRS continue d'en suivre le comportement, au chapitre des droits de la personne, par des évaluations annuelles.

Tel que prévu au sous-alinéa 38a)(iii) de la *Loi sur le SCRS*, le CSARS examine ces ententes et contrôle l'information et les renseignements échangés. Cette année, il a choisi d'examiner les relations du SCRS avec des organismes de quatre pays soupçonnés de violer les droits de la personne.

Méthode

Cette étude a porté sur les ententes conclues par le SCRS avec sept organismes étrangers et sur l'information échangée à la faveur de ces ententes.

Contexte

Le CSARS a examiné une enquête de contre-espionnage de longue durée dont la dernière étude remontait à 1996. Un service de renseignement étranger était soupçonné d'activités secrètes d'espionnage et d'ingérence au Canada, selon les définitions des alinéas 2a) et b) de la *Loi sur le SCRS*.

Le SCRS a cherché à déterminer quels secteurs ou industries (aéronautique, télécommunications, militaire, scientifique ou technologique) étaient ciblés par le service de renseignement étranger. Il s'est aussi penché sur des incidents d'espionnage présumé à l'endroit d'expatriés venus s'installer au Canada.

Méthode

Le CSARS a concentré son examen sur la gestion de cette enquête du Service entre janvier 2002 et décembre 2004, et sur certains documents débordant cette période. Cela comprend les documents, versions papier et électronique, ayant trait aux décisions d'enquêter et à la gestion des sources humaines.

Constatations

Dans l'ensemble, l'enquête de contre-espionnage était conforme à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle au cours de la période étudiée. Le CSARS a conclu que :

- le SCRS avait des motifs raisonnables de soupçonner ce service de renseignement étranger ou ses agents de présenter une menace pour la sécurité du Canada;
- le niveau et le degré d'intrusion de l'enquête allaient de pair avec cette menace;
- le Service avait recueilli uniquement des informations strictement nécessaires pour remplir son mandat.

L'alinéa 2b) définit ainsi l'ingérence étrangère : « les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque ».

Selon l'alinéa 2a) de la *Loi sur le SCRS*, « l'espionnage... visant le Canada ou [préjudiciable] à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage » sont des menaces envers la sécurité du Canada.

Le CSARS s'est vu fournir toutes les évaluations de la menace effectuées par le CIESN entre février 2003 et juillet 2004, et celles émanant du CIEEM entre octobre 2004 et février 2005. Parmi ces documents, il a examiné un échantillon des rapports du CIESN et du CIEEM afin de voir si les processus de rédaction, d'examen et de distribution étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle.

Constations

Le CSARS a constaté que, dans l'ensemble, le Service avait respecté la *Loi* et les instructions ministérielles. Cependant, il a aussi constaté que le SCRS n'avait pas encore intégré les opérations du Centre dans les politiques opérationnelles existantes, ni approuvé de nouvelles politiques particulières au CIEEM. **Le CSARS a recommandé que le SCRS examine ses politiques pour déterminer les modifications particulières qui s'imposent à l'égard du CIEEM afin de tenir compte du rôle de cet organisme.**

Le CIEEM effectue des évaluations qui servent à prévenir le gouvernement des menaces terroristes contre le Canada et les intérêts canadiens à l'étranger. Il consulte ses partenaires et clients afin de déterminer des sujets particuliers, de même qu'un comité consultatif en vue d'élaborer son plan de travail. Chaque évaluation intègre les renseignements émanant de sources ouvertes et classifiés, reçus de divers organismes canadiens et étrangers. Le personnel du CIEEM puise les renseignements classifiés sur place, aux réseaux électroniques propres à chacun des organismes partenaires, qui contiennent des renseignements secrets en matière de criminalité et d'immigration. Le CSARS a constaté que la capacité électronique du CIEEM lui confère un accès sans précédent et poussé aux sources canadiennes du renseignement.

Une fois que le CIEEM a terminé ses évaluations de la menace, il les distribue aux ministères et organismes fédéraux, provinciaux et territoriaux et à ceux des administrations municipales ainsi qu'aux organismes canadiens d'exécution de la loi. Il les transmet aussi à des organismes étrangers. Le CSARS a constaté que la plupart de ces échanges avaient eu lieu à la faveur d'accords autorisés pour la coopération du Service avec des services de sécurité et de renseignement étrangers. Il a toutefois noté que le SCRS échangeait de l'information avec un autre centre de fusion étranger sans avoir conclu d'accord en vertu de l'article 17, comme le prescrit la *Loi sur le SCRS*. **Le Comité a recommandé que le SCRS officialise sa relation avec ce centre étranger et fasse approuver une entente avec celui-ci par le ministre de la Sécurité publique.**

Le CIEEM transmet aussi, au sein du gouvernement du Canada, les évaluations de la menace émanant de ses pendants aux États-Unis, au Royaume-Uni, en Australie et en Nouvelle-Zélande. Ces évaluations comptent pour près des trois quarts de tous les rapports que le CIEEM a distribués entre octobre 2004 et août 2005. Le CSARS a mentionné que le CIEEM avait entrepris d'analyser les problèmes de distribution en janvier 2005 et qu'il scrutait son réseau pour déceler les goulets d'étranglement.

Examen du Centre intégré d'évaluation des menaces

Rapport n° 2005-03

Contexte

En avril 2004, le gouvernement du Canada a annoncé *Protéger une société ouverte : la politique canadienne de sécurité nationale*. L'un des effets de cette politique a été la création du Centre intégré d'évaluation des menaces (CIEM), en juillet 2004, visant à assurer la transmission rapide des évaluations de menaces terroristes aux décideurs qui en ont besoin. L'inauguration du Centre a eu lieu en octobre 2004.

Le CIEM, qui a ses bureaux à l'administration centrale du SCRS, permet aux autorités municipales et provinciales de participer davantage à évaluer et à contourner les menaces à la sécurité du Canada. Il est un élément fonctionnel du Service et est assujéti à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle du Service, ainsi qu'à la surveillance du CSARS.

Méthode

Cet examen visait à servir de base à de futures études du CSARS. Celui-ci a examiné tous les documents disponibles concernant la formation et les opérations du CIEM et de son prédécesseur, le Centre intégré d'évaluation de la sécurité nationale (CIESN).

Le CIEM réunit des analystes, des experts en sécurité et des responsables de l'exécution de la loi et du renseignement de l'Agence des services frontaliers du Canada, du Centre de la sécurité des télécommunications, du ministère de la Défense nationale, d'Affaires étrangères Canada, du Bureau du Conseil privé, du ministère de la Sécurité publique, de Transports Canada, de la Police provinciale de l'Ontario, de la Sûreté du Québec, de la GRC et du SCRS.

Bien des membres de la collectivité de la sécurité et du renseignement ont adopté le terme « centres de fusion » pour désigner l'intégration de toute l'information qui a trait à la sécurité et à la défense d'un pays.

Le CSARS a formulé cinq recommandations.

Premièrement, le Comité a repris une recommandation de son rapport sur Maher Arar en vertu de l'article 54, soit que les agents de liaison-sécurité du SCRS conservent par écrit les demandes d'information de l'Administration centrale du SCRS qu'ils transmettent verbalement aux services de renseignement étrangers.

Les quatre autres recommandations concernent les questions ayant trait aux documents qu'emploie le SCRS pour gérer ses relations avec l'étranger.

Le Comité a recommandé que le SCRS mette à jour le profil du bureau.

Pour assurer que l'Administration centrale du SCRS et les ALS soient au courant des informations échangées avec leurs partenaires étrangers, la politique opérationnelle prescrit aux employés du SCRS de présenter un rapport écrit après avoir visité un représentant d'un service étranger ou pris contact avec lui. Non seulement ces rapports sont-ils importants pour la gestion des relations du SCRS avec l'étranger, mais ils tiennent les ALS compétents au fait des discussions tenues avec les organismes étrangers et de l'information qui a été échangée avec leurs homologues étrangers. Au cours de la période étudiée, le bureau n'a pas remis ces rapports régulièrement à l'Administration centrale du SCRS. Le CSARS a recommandé que l'Administration centrale du SCRS rappelle aux directions opérationnelles et aux ALS de présenter ces rapports promptement.

Le Comité a aussi recommandé que le SCRS établisse un document d'évaluation d'une nouvelle relation avec un organisme étranger donné, en particulier parce que l'Administration centrale du SCRS avait formulé la même requête en 2003.

Enfin, en ce qui a trait aux documents du SCRS concernant une entente distincte et relativement nouvelle avec un service de renseignement particulier, le Comité a signalé l'absence de tout document concernant des préoccupations qu'auraient exprimées, à l'égard des droits de la personne, des organisations telles qu'Amnistie internationale et Human Rights Watch. En conséquence, le CSARS a recommandé que le SCRS élabore une politique opérationnelle concernant la documentation de ses relations avec les organismes qui sont connus pour leurs violations des droits de la personne ou auxquels on attribue de tels gestes.

Liaison du SCRS avec des organismes étrangers : examen d'un bureau de liaison-sécurité

Rapport n° 2005-02

Contexte

Le SCRS a un certain nombre de bureaux d'agent de liaison-sécurité (ALS) en dehors du Canada. Les emplacements de ces bureaux sont classifiés, mis à part ceux de Washington, Londres et Paris. Cette année, le CSARS a examiné l'un des plus occupés de ces bureaux qui reçoit chaque année des milliers de messages et a de nombreux échanges avec les services de sécurité et de renseignement du pays concerné.

Méthode

L'objectif du Comité était de déterminer si les échanges d'information de ce bureau avec des organismes étrangers respectaient la portée des ententes de liaison approuvées. Le CSARS en a aussi évalué les activités pour établir si elles étaient conformes à la Loi sur le SCRS et aux instructions ministérielles ainsi qu'à la politique et à la procédure opérationnelles du Service.

Le CSARS a effectué cette étude en examinant les documents à l'Administration centrale du SCRS et en visitant ce bureau à quelques reprises. Pour la mise en contexte, le rapport tient aussi compte des tendances relevées lors de précédents examens de bureaux d'ALS et à l'occasion des études continues du CSARS sur les ententes du SCRS avec des organismes étrangers.

Constatations

Le Comité a constaté que le bureau d'ALS en question était géré efficacement et que ses opérations étaient conformes à la Loi sur le SCRS et aux instructions ministérielles ainsi qu'à la politique opérationnelle et aux directives du Service.

Les ALS :

- assurent la liaison courante avec les services étrangers de renseignement de sécurité;
- fournissent des services de filtrage de sécurité à l'appui du programme d'immigration du Canada;
- effectuent des échanges de renseignements de sécurité avec les organismes approuvés;
- conseillent les cadres supérieurs de la mission ou de l'ambassade canadienne.

Le CSARS s'est inquiété d'un échange d'information auquel avait pris part un organisme étranger et il a relevé un problème découlant du mauvais usage de l'information du SCRS par un partenaire canadien.

Le CSARS a aussi appris que l'enquête du SCRS sur l'organisation terroriste l'avait mis en rapport avec une institution canadienne névralgique.

Le CSARS a pour mandat d'enquêter sur les menaces à la sécurité du Canada, aussi névralgiques que soient les scènes où elles se manifestent. Néanmoins, de par certaines instructions ministérielles et politiques opérationnelles, le Service est tenu de prendre un soin particulier s'il est possible que ses activités d'enquête le mettent en rapport avec une institution canadienne névralgique, terme qui englobe le secteur universitaire, politique, religieux et syndical et celui des médias.

Conformément à l'article 2 de la *Loi sur le SCRS*, lorsqu'il scrute des activités qui menacent la sécurité du Canada, le SCRS ne peut enquêter sur celles qui comportent des actes licites de défense d'une cause, de protestation ou de manifestation d'un désaccord, sauf si ces actes sont posés parallèlement aux activités menaçantes. Cependant, en certaines occasions, il enquête sur des groupes ou des individus qui se livrent à la fois à une activité politique licite et à une autre qui est liée à la menace; qui exercent une activité liée à la menace sous couvert d'une activité politique licite; ou qui exercent une activité politique licite qui dégénère en activité liée à la menace.

Ces politiques sont plus rigoureuses que celles visant les autres aspects des opérations du SCRS. Elles obligent celui-ci à faire la part entre le recours à des méthodes d'enquête intrusives et le préjudice qui peut en découler à l'égard des libertés civiles ou de ces institutions sociales fondamentales. Cette étude a révélé un secteur où, de l'avis du CSARS, il faudrait élargir la politique opérationnelle afin d'englober les rapports du SCRS avec le secteur canadien en question.

En conséquence, le Comité a recommandé que le SCRS élargisse sa politique relative aux secteurs névralgiques de manière à exiger que certaines techniques d'enquête soient autorisées par la haute direction. Il est utile de mentionner que le CSARS a fait une recommandation semblable dans son rapport annuel de l'an dernier (voir l'étude du CSARS n° 2004-06).

Examen d'une enquête antiterroriste

Rapport n° 2005-01

Contexte

Cette étude concerne une enquête menée par le SCRS sur une organisation terroriste soupçonnée de recruter au Canada des fonds destinés à ses activités à l'étranger.

Méthode

Le CSARS a examiné cette enquête pour la période du 1^{er} janvier 2004 au 31 janvier 2005. Il a étudié les documents, en versions électronique et imprimée, qui avaient trait aux activités opérationnelles suivantes du Service :

- ciblage d'individus soupçonnés d'exercer des activités liées à la menace et processus d'autorisation d'enquête;
- direction de sources humaines contre les sources autorisées;
- tous les échanges d'information avec les partenaires étrangers;
- conseils donnés au gouvernement.

Constatations

Dans l'ensemble, les activités du Service étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et à la politique opérationnelle au cours de la période étudiée. Le CSARS a constaté que le Service avait des motifs raisonnables de soupçonner les cibles d'enquête de constituer une menace pour la sécurité du Canada et que les autorisations d'enquête allaient de pair avec la gravité des menaces. Les enquêteurs du Service ont recueilli uniquement des informations strictement nécessaires à l'enquête.

De plus, le recours à des sources humaines par le Service et ses échanges d'information avec des partenaires canadiens étaient conformes à la *Loi sur le SCRS* et aux instructions ministérielles applicables. Il y a eu quelques erreurs administratives dans la gestion des sources par le SCRS, mais elles n'ont pas affecté la qualité de l'enquête. Le Comité ne les a pas, non plus, perçues comme graves. Il a aussi constaté que tous les rapports distribués par le SCRS aux principaux représentants du gouvernement reflétaient fidèlement l'information trouvée dans les rapports opérationnels du Service.

Le programme de recherche du CSARS est conçu de manière à englober un vaste éventail de sujets. Lorsqu'il décide des études à mener, le Comité tient compte :

- des priorités et préoccupations exposées par le Parlement ou dans les médias;
- des activités particulières qui pourraient porter atteinte aux droits et libertés individuels;
- du rapport classifié présenté au Ministre par le directeur du SCRS;
- de la nécessité d'évaluer régulièrement chacune des directions opérationnelles du Service et chacun de ses bureaux régionaux;
- des pouvoirs que confère au Service la *Loi sur le SCRS*, selon les détails qu'on y trouve;
- des événements susceptibles de présenter une menace à la sécurité du Canada;
- des engagements du CSARS à réexaminer des questions particulières;
- des questions cernées par le Comité dans l'exercice de sa fonction relative aux plaintes;
- des orientations stratégiques ou initiatives nouvelles annoncées par le SCRS ou par le gouvernement du Canada.

Cette approche permet au Comité de gérer le risque inhérent de ne pouvoir examiner qu'un faible pourcentage des activités du SCRS une année donnée. Chaque étude donne un « instantané » des actions du Service par rapport aux lois, politiques et instructions ministérielles applicables. Depuis deux décennies, les études du CSARS fournissent au Parlement et aux Canadiens un tableau complet des activités opérationnelles du Service et l'assurance que les actions de celui-ci sont conformes à la loi.

Le Comité est l'un des divers mécanismes qui sont conçus pour assurer la reddition de comptes du SCRS. Celui-ci doit en outre faire rapport de ses opérations par l'entremise de l'appareil gouvernemental en place, notamment le ministre de la Sécurité publique, l'inspecteur général du SCRS, les organismes centraux et le vérificateur général ainsi que les commissaires à l'information et à la protection de la vie privée du Canada.

A. Examen des activités de renseignement de sécurité du SCRS

EXERCICE DE SA FONCTION DE SURVEILLANCE PAR LE CSARS

Le Comité de surveillance des activités de renseignement de sécurité est le seul organisme indépendant, de l'extérieur, à être habilité par la loi et à avoir l'expertise voulue pour examiner les activités du SCRS. Il a été créé en vertu de la *Loi sur le SCRS* (1984) afin d'assurer au Parlement du Canada et aux Canadiens que le Service respecte la loi, les politiques et les instructions ministérielles dans l'exercice de ses fonctions. Ce faisant, le CSARS s'emploie à veiller au respect des droits fondamentaux et des libertés des Canadiens.

Pour remplir son mandat, le Comité confie chaque année à son personnel diverses études qui fournissent un examen rétrospectif et une évaluation d'enquêtes et de fonctions particulières du SCRS. La *Loi sur le SCRS* lui confère des pouvoirs quasi illimités pour ce qui est de scruter le rendement du Service, Exception faite des seuls renseignements confidentiels du Cabinet, le CSARS a le pouvoir absolu d'examiner toute information touchant les activités du SCRS, quel qu'en soit le niveau de classification.

Le rapport de chaque étude contient des constatations et des recommandations du Comité. Une fois terminé, il est présenté au directeur et à l'inspecteur général du SCRS.

En vertu de l'article 54 de la *Loi sur le SCRS*, le CSARS est en outre autorisé à présenter au ministre de la Sécurité publique un rapport spécial sur toute question que ses membres estiment revêtir une importance particulière, ou tout rapport spécial que le Ministre lui demande.

En quoi un organisme de contrôle diffère-t-il d'un organisme de surveillance?

Un organisme de contrôle suit en permanence ce qui se passe au sein d'un service de renseignement et il a pour mandat d'évaluer les enquêtes en cours ou le travail « en temps réel ». Le CSARS est un organisme de surveillance de sorte que, contrairement à un organe de contrôle, il peut évaluer pleinement le rendement passé du SCRS sans être mêlé d'aucune manière à ses décisions et activités courantes d'ordre opérationnel.

Section 1

Bilan de l'exercice 2005-2006

Le Comité de surveillance des activités de renseignement de sécurité fournit au Parlement du Canada, et par son entremise aux Canadiens, l'assurance que le Service canadien du renseignement de sécurité (SCRS) respecte la loi dans l'exercice de ses fonctions. Le CSARS a deux fonctions principales. La première consiste à mener des études approfondies sur les activités du Service pour vérifier si elles sont conformes à la *Loi sur le Service canadien du renseignement de sécurité (Loi sur le SCRS)* et aux divers instruments stratégiques qui en découlent, ainsi qu'aux instructions du ministre de la Sécurité publique. La seconde consiste à recevoir les plaintes que toute personne peut porter à l'égard des activités du Service et à faire enquête à ce sujet.

Le rapport annuel de 2005-2006 du CSARS est agencé en fonction des principales constatations et recommandations qui découlent de ses études et de ses enquêtes sur les plaintes. On y trouve aussi les renseignements plus généraux qu'il recueille pour informer ses membres et aider le lecteur à saisir le contexte plus vaste dans lequel baigne le travail du SCRS en matière de renseignement de sécurité. Voici un résumé des trois sections du rapport :

Section 1 : bilan de l'exercice 2005-2006

Cette section résume sept examens que le CSARS a effectués pendant la période visée par le présent rapport. Elle fournit aussi de l'information sur les plaintes qu'il a reçues.

Section 2 : mécanismes redditionnels du SCRS

Cette section décrit le cadre de politiques et de régie à l'intérieur duquel le SCRS exerce ses fonctions. Elle expose aussi les renseignements que le Service fournit au sujet de ses activités, plans et priorités opérationnels, et cela, par rapport à ses principales directions.

Section 3 : voulez-vous en savoir plus long sur le CSARS?

Cette section fournit des détails sur les activités du Comité en matière de collecte d'information, de rayonnement, de liaison et d'administration, y compris le budget annuel et les dépenses du CSARS.

détroge aux règles confirme les pires préjugés et soupçons de ses ennemis, alors que les droits individuels sont dénués de sens sans une sécurité véritable et durable pour la personne. Voilà pourquoi il est si important que les corps policiers et les organismes de sécurité nationale soient tenus de rendre compte de leurs actions et de leurs choix.

Depuis vingt-deux ans, le CSARS s'emploie à assurer une reddition de comptes véritable en défendant les droits fondamentaux et les libertés des Canadiennes et des Canadiens en insistant pour que le SCRS respecte la loi dans ses actions. Voilà notre héritage au Parlement et aux citoyens que nous servons et notre engagement indéfectible à leur égard.

Le rapport de cette année met aussi en relief des procédures innovatrices destinées à moderniser la fonction relative aux plaintes. Dans le but de mieux répondre aux besoins, nous avons affiché une traduction arabe de « Comment porter plainte » sur le site Web du CSARS. En consultation avec le SCRS, nous avons instauré les conférences préparatoires aux audiences afin de résoudre les questions de procédure préliminaires et nous avons adopté le principe de la production continue de façon que de nouveaux documents puissent être déposés en tout temps avant qu'une décision soit rendue. Nous sommes fiers de ces innovations, car elles ont rationalisé notre processus d'enquête et, avec le temps, elles concourront à une meilleure compréhension du mécanisme de recours du CSARS.

La reddition de comptes est la raison d'être des organismes de surveillance et de contrôle du monde entier. Voilà pourquoi nous estimions si important de prendre part aux travaux de la Commission O'Connor, chargée de faire des recommandations au sujet d'un organisme indépendant qui aurait pour rôle d'examiner les activités de la GRC ayant trait à la sécurité nationale. Au cours de la dernière année, notre président a discuté de la question lors d'une audience publique de la Commission, et les membres du personnel du CSARS ont tenu de vastes discussions avec leurs homologues de la Commission. Il est probable que les recommandations du juge O'Connor polariseront sensiblement l'attention du public sur la pertinence des mécanismes de surveillance du Canada et nous brûlerons de connaître la réaction du gouvernement fédéral.

Comme nous l'avons dit plus tôt, le terrorisme est la source de défis d'envergure constants pour le Canada et pour les autres démocraties occidentales. Notre appartenance à une société libre nous contraint à recourir à toutes les ressources dont nous disposons pour faire échec à cette menace meurtrière, tout en soutenant les principes de la responsabilité, de la justice, du respect des droits individuels et de la conformité absolue à la règle de droit.

durable pour la personne.

S'il est un message que nous pouvons laisser au lecteur, c'est qu'il ne faut pas supposer l'existence d'un conflit insoluble entre les exigences de la sécurité du public et nos valeurs démocratiques. En réalité, il faut plutôt y voir une complémentarité. Une société qui

Au tournant du XXI^e siècle, le spectre du terrorisme est devenu la préoccupation centrale des forces de police et des organismes qui veillent sur la sécurité nationale. Même dans les pays épargnés par les attaques directes, le terrorisme a suscité la peur et l'incertitude. Pour le Canada, le défi consiste à assurer la sécurité du public sans compromettre les valeurs qui sont les assises de notre tradition démocratique.

Le Comité de surveillance des activités de renseignement de sécurité (CSARS) est l'une des entités qui ont charge d'assurer cet équilibre. Il est le seul organisme indépendant, de l'extérieur, à être habilité à surveiller les activités du Service canadien du renseignement de sécurité (SCRS), en examinant ses opérations et en enquêtant sur les plaintes. Depuis plus de deux décennies, le CSARS s'acquitte de cette responsabilité, toujours conscient du rôle vital du SCRS dans la sauvegarde de notre société, mais vigilant à l'égard des pouvoirs extraordinaires qu'il est autorisé à exercer.

Dans la mesure où la sécurité nationale le permet, notre rapport annuel résume les principales réalisations du CSARS en 2005-2006. Le rapport de cette année expose les faits saillants de sept études et de quatre décisions rendues dans des dossiers de plaintes. Au nombre des études les plus dignes de mention figure celle sur les relations du SCRS avec des organismes de quatre pays soupçonnés d'avoir violé les droits de la personne, outre notre premier examen du Centre intégré d'évaluation des menaces, élément clé de la Politique canadienne de sécurité nationale. Nous avons aussi examiné les techniques de surveillance électronique et de collecte d'information du SCRS afin de mieux comprendre comment les technologies en évolution rapide sont employées par le SCRS et exploitées par les terroristes et les services de renseignement étrangers. Ces sept études nous ont amenés à formuler 14 recommandations qui sont résumées à la fin du présent rapport.

En plus d'effectuer des études, le CSARS est aussi chargé d'enquêter sur les plaintes contre le SCRS. En jouant ce rôle, nous assurons un mécanisme de recours indépendant aux groupes et aux individus, avec tous les pouvoirs d'une cour supérieure. Au fil des deux dernières décennies, le CSARS a rendu 125 décisions au sujet de plaintes, dont chacune témoigne de notre justice et de notre objectivité. En 2005-2006, le CSARS a traité 63 plaintes, ce qui représente une forte hausse par rapport aux dernières années, et il a rendu quatre décisions nouvelles. L'une d'elles concerne une plainte portée en vertu de l'article 42, au sujet du refus d'une habilitation de sécurité à M. Bhupinder Liddar, et le CSARS y a tranché en faveur du plaignant.

Section 2 : mécanismes redactionnels du SCRS	29
A. Exigences en matière de rapports	31
Rapport annuel du directeur du SCRS (2004-2005)	31
Certificat de l'inspecteur général (2005)	32
Agissements illicites de la part du SCRS	32
Communication d'informations	33
B. Ententes en vertu de l'article 17	34
Ententes avec des organismes canadiens	34
Ententes avec des organismes étrangers	35
C. Cadre de politiques et de régie	36
Exigences nationales en matière de renseignement de sécurité	36
Instructions ministérielles	37
Modifications à la politique opérationnelle du SCRS	37
Règlements et nominations par le gouverneur en conseil	37
D. Activités opérationnelles du SCRS	38
Direction du contre-espionnage	38
Direction de la lutte contre la prolifération	39
Direction de l'antiterrorisme	40
Direction de la recherche, de l'analyse et de la production	41
Direction du filtrage de sécurité	42
Direction de la liaison avec l'étranger et des visites	48
Mandats de la Cour fédérale : généralités et statistiques	49
Centre intégré d'évaluation des menaces	51
Section 3 : voulez-vous en savoir plus long sur le CSARS?	53
Composition du Comité	55
Personnel et organisation	56
Budget et dépenses	57
Demandaes en vertu des Lois sur l'accès à l'information et sur la protection des renseignements personnels	57
Communications	58
Fonction de contrôleur moderne	59
Annexe A : examens du CSARS depuis 1984	61
Annexe B : recommandations	75

Table des matières

Déclaration du Comité	v
Agencement du rapport	viii

Section 1 : bilan de l'exercice 2005-2006

A. Examen des activités de renseignement de sécurité du SCRS

Exercice de sa fonction de surveillance par le CSARS	3
Examens du CSARS en 2005-2006	5
Examen d'une enquête antiterroriste (n° 2005-01)	5
Liaison du SCRS avec des organismes étrangers :	
examen d'un bureau de liaison-sécurité (n° 2005-02)	7
Examen du Centre intégré d'évaluation des menaces (n° 2005-03)	9
Examen d'une enquête de contre-espionnage (n° 2005-04)	11
Examen des ententes conclues avec des pays soupçonnés de violer les droits de la personne (n° 2005-06)	12
Examen des techniques de surveillance électronique et de collecte d'information du SCRS (n° 2005-07)	15
Examen des activités et enquêtes dans une région du SCRS (n° 2005 08)	17

B. Enquêtes sur les plaintes

Procédure d'enquête du CSARS sur les plaintes	18
Nouvelle procédure	22
Décisions du CSARS sur les plaintes en 2005-2006	22
Rapport de l'enquête sur la plainte portée dans l'affaire Bhupinder Liddar (rapport n° 1)	22
Refus d'une habilitation de sécurité (rapport n° 2)	23
Discrimination présumée (rapport n° 3)	25
Présumée réaction inappropriée à la maladie d'un plaignant (rapport n° 4)	26

Le 29 septembre 2006


L'honorable Stockwell Day, C.P., député
Ministre de la Sécurité publique
Chambre des communes
Ottawa (Ontario)
K1A 0A6


Monsieur le Ministre,

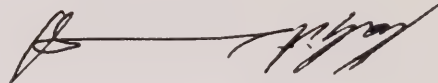
Conformément à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, nous présentons au Parlement, par votre entremise, le rapport du Comité de surveillance des activités de renseignement de sécurité pour l'exercice 2005-2006.


Vous agréer, Monsieur le Ministre, l'expression de notre haute considération.

Le Président,


Gary Filmon, C.P., O.M.


Roy Romanow, C.P., O.C., C.R.


Baljit S. Chadha, C.P.
Raymond A. Speiser
Raymond Speaker, C.P., O.C.


Alda Landry, C.P., C.M., C.R.

Les membres du CSARS (de gauche à droite) : l'honorable Baljit S. Chadha, l'honorable Gary Filmon (président), l'honorable Raymond Speaker, l'honorable Aldea Landry et l'honorable Roy Romanow



Photo : Couvrette/Ottawa

Examen opérationnel du Service
canadien du renseignement de sécurité

Rapport annuel du CSARS 2005-2006



Comité de surveillance des activités de renseignement de sécurité
B.P. 2430, succursale D
Ottawa (Ontario)
K1P 5W5

Téléphone : 613-990-8441

Télécopieur : 613-990-5230

www.sirc-csars.gc.ca

Les appels à frais virés sont acceptés de 8 h à 17 h, heure normale de l'Est.

Nota : aux fins du présent document, la forme masculine désigne, s'il y a lieu, aussi bien les femmes que les hommes.

© Travaux publics et Services gouvernementaux Canada 2006

N° de cat. PS105-2006

ISBN 0-662-49440-7

Examen opérationnel du Service
canadien du renseignement de sécurité


Rapport annuel du CSARS 2005-2006

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ



CA1
SIR
- A56

SECURITY INTELLIGENCE
REVIEW COMMITTEE



SIRC Annual Report 2006–2007

An operational review of the
Canadian Security Intelligence Service

Canada



Security Intelligence Review Committee
P.O. Box 2430, Station “D”
Ottawa ON
K1P 5W5

(613) 990-8441 (voice)

(613) 990-5230 (fax)

www.sirc-csars.gc.ca

Collect calls are accepted between 8:00 AM and 5:00 PM, EST

© Public Works and Government Services Canada 2007

Cat. No. PS105-2007

ISBN 978-0-662-05006-3



SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2006–2007

**An operational review of the
Canadian Security Intelligence Service**





Members of SIRC (from left to right):
The Honourable Baljit S. Chadha, The Honourable Gary Filmon (Chair), The Honourable
Raymond Speaker, The Honourable Aldéa Landry, The Honourable Roy Romanow

September 28, 2007

The Honourable Stockwell Day, P.C., M.P.
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6


Dear Minister:

As required by Section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 2006–07, for your submission to Parliament.

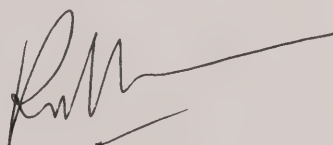
Yours sincerely,



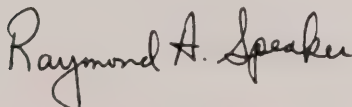
Gary Filmon, P.C., O.M.
Chair



Baljit S. Chadha, P.C.



Roy Romanow, P.C., O.C., Q.C.



Raymond Speaker, P.C., O.C.



Aldéa Landry, P.C., C.M., Q.C.

Table of contents

Members' Statement	v
How this report is organized	vii
Section 1: A year in review 2006–07	1
A. Review of CSIS security intelligence activities	3
How SIRC carries out its review function	3
Review of a security liaison post (2006–01)	5
Review of activities and investigations in a CSIS regional office (2006–02)	6
Review of a counter-terrorism investigation (2006–03)	7
Review of a Section 16 activity (2006–04)	9
Review of a counter-terrorism investigation (2006–05)	11
Review of CSIS's collaboration and exchanges of intelligence post-9/11 (2006–06)	12
Review of security screening outside of the federal government (2006–07)	14
Review 2006–08	16
Review of the CSIS Counter Espionage Investigations desk (2006–09)	16
B. Section 54 Report	18
Review of the case of Mohammed Mansour Jabarah (2005–05) ...	18
C. Investigation of complaints	23
How SIRC investigates complaints	23
How SIRC determines jurisdiction of a complaint	26
D. SIRC complaint decisions 2006–07	27
Alleged discrimination in an immigration process (2006–01)	27
Alleged actions by CSIS during a citizenship interview (2006–02) ..	28
Revocation of a security clearance (2006–03)	28
Alleged false statements (2006–04)	29
Alleged delay in processing a citizenship application (2006–05) ...	30

Section 2: CSIS accountability mechanisms	33
A. Reporting requirements	35
CSIS Director's Annual Report (2005–06)	35
Certificate of the Inspector General of CSIS (2006)	36
Unlawful conduct by CSIS	38
Disclosures of information	38
B. Foreign and domestic arrangements	39
Arrangements with domestic agencies	39
Arrangements with foreign agencies	39
C. Policy and governance	41
National Requirements for Security Intelligence	41
Ministerial Direction	42
Changes in CSIS operational policy	42
Governor-In-Council regulations and appointments	42
D. CSIS operational activities	43
1. Intelligence	44
Security Screening Branch	44
Intelligence Assessments Branch	50
Human Sources and Operations Support Branch	50
Scientific and Technical Services	50
Integrated Threat Assessment Centre	50
2. Operations	51
International Terrorism Branch	51
Middle East and Africa Branch	51
Asia, Europe and Americas Branch	51
International Region	52
Federal Court warrants and warrant statistics	52
Section 3: About SIRC	55
Committee membership	57
SIRC meetings and briefings 2006–07	57
Staffing and organization	58
Budget and expenditures	59
Inquiries under the <i>Access to Information and Privacy Acts</i>	59
Communications	59
Management accountability	60
Appendix A: SIRC reviews since 1984	63
Appendix B: Recommendations	77

Members' Statement

This year marks a significant anniversary in Canada's history. A quarter of a century has passed since the signing of the *Canadian Charter of Rights and Freedoms*, a document that guarantees freedom of conscience and religion; freedom of thought, belief, opinion and expression, including freedom of the press; freedom of peaceful assembly; and freedom of association. With the adoption of the *Charter*, these freedoms became constitutionally protected and Canadians gained recourse to the courts if the state infringed upon or denied their *Charter* rights.

There is no question that the bedrock values articulated in that historic constitutional document have helped to define what it means to be Canadian. They have had a profound influence on government, including the work of review agencies such as the Security Intelligence Review Committee (SIRC). These freedoms have been brought into sharp relief in recent years when considered along with the state's obligation to protect the safety of its citizens against a growing terrorist threat.

In carrying out our duties, the Committee has often found itself considering *Charter* issues. For example, as part of our reviews, we regularly examine CSIS's execution of judicially authorized warrant powers to ensure that intrusive investigative techniques comply with the law and the terms of the Court, and therefore do not constitute unreasonable search and seizure.

SIRC recognizes that the conduct of security intelligence agencies can prompt impassioned debate about whether the ends can ever justify the means. We also have first-hand knowledge that there are individuals who will seek to exploit Canada's rights and freedoms in order to harm our country, our citizens and our neighbours and friends around the world.

It is against this backdrop that SIRC's annual report features a summary of a Section 54 report that was submitted to the Minister of Public Safety on August 17, 2007. This type of report is relatively rare: only eight have been prepared in the last ten years. This latest report deals with the case of Mohammed Mansour Jabarah, a Canadian citizen and an admitted al Qaida member, who was convicted of terrorist-related offences in the United States.

In reviewing CSIS's role in this matter, we found that some of its actions violated certain rights as guaranteed under the *Charter*. As a result, we have made several recommendations to the Minister of Public Safety and the CSIS Director.

It is important to understand why SIRC takes issue with some of CSIS's actions and we invite readers to consider our analysis carefully. Mohammed Mansour Jabarah is a Canadian who, no matter how heinous his crimes and no matter how much we deplore them, is entitled to all of the rights and freedoms afforded to any other citizen under our *Charter*. Furthermore, an agent of the state must uphold the *Charter* otherwise Canadian officials would be free to pick and choose to whom certain guaranteed rights and freedoms would apply. Clearly, that would be unacceptable to all Canadians.

"An agent of the state must uphold the *Charter* otherwise Canadian officials would be free to pick and choose to whom certain guaranteed rights and freedoms would apply."

SIRC recognizes that police and security intelligence agencies in the post 9/11 world must deal with daunting challenges, including globalized and technologically sophisticated terrorist groups. We also know that the relative safety that Canadians enjoy is thanks in large part to the efforts of these same agencies on our behalf. But the obligation to ensure public safety ought not to reduce in any way respect for the rule of law.

Mr. Justice Ian Binnie of the Supreme Court of Canada characterized the competing demands of national security and human rights as a "clash of titans." It is true that at times, human rights and national security objectives may appear to clash. But in a healthy democracy where rights and freedoms have constitutional protection, we firmly believe that they can—indeed they must—coexist. That is a principle which all Canadians should uphold and that every citizen has a continuing responsibility to protect.

How this report is organized

The Security Intelligence Review Committee provides assurance to the Parliament of Canada—and through it, to Canadians—that CSIS is acting lawfully in the performance of its duties. SIRC has two key functions. The first is to conduct in-depth reviews of CSIS activities to ensure that they accord with the *CSIS Act* and the various policy instruments that flow from it, and with direction from the Minister of Public Safety. The second is to receive and investigate complaints by any person about any action of the Service.

SIRC's 2006–07 annual report is organized to reflect key findings and recommendations arising from its reviews and complaints investigations. Also included is more general background material, collected to inform Committee Members and to assist readers in understanding the broader context in which CSIS's security intelligence work is carried out. The report's three sections are:

Section 1: A year in review 2006–07

This section summarizes nine reviews SIRC completed during the period covered by this report. It also provides information about five complaint reports issued by SIRC.

Section 2: CSIS accountability mechanisms

Featured in this section are descriptions of the policy and governance framework within which CSIS operates. This section also contains information provided by CSIS on operational activities, plans and priorities, organized according to the Service's major branches.

Section 3: About SIRC

This section provides details about the outreach, liaison and administrative activities of SIRC, including its annual budget and expenditures.

Section 1

A year in review 2006–07

A year in review 2006–07

A. Review of CSIS security intelligence activities

HOW SIRC CARRIES OUT ITS REVIEW FUNCTION

The Security Intelligence Review Committee is the only body with the legal mandate and expertise to carry out ongoing, independent review of the activities of CSIS. SIRC was established under the *CSIS Act* (1984) to provide assurance to the Parliament of Canada and to Canadians that CSIS is acting in accordance with the law, policy and Ministerial Direction in the performance of its duties and functions. In doing so, SIRC seeks to ensure that CSIS respects the fundamental rights and freedoms of Canadians.

To fulfill its mandate, SIRC directs staff to undertake a number of reviews each year. These provide a retrospective examination and assessment of specific CSIS investigations and functions. Under the *CSIS Act*, SIRC has virtually unlimited power to review CSIS's performance. With the sole exception of Cabinet confidences, SIRC has the absolute authority to examine all information concerning CSIS's activities, no matter how highly classified that information may be.

Each review includes SIRC's findings and recommendations. Upon completion, the report is forwarded to the Director of CSIS and the Inspector General of CSIS.

SIRC is also authorized under Section 54 of the *CSIS Act* to provide special reports to the Minister of Public Safety on any matter that the Committee identifies as having special importance or that the Minister directs SIRC to undertake.

What's the difference between an oversight and a review agency?

An oversight body looks on a continual basis at what is taking place inside an intelligence service and has the mandate to evaluate and guide current investigations or work in "real time." SIRC is a review body, so unlike an oversight agency, it can make a full assessment of CSIS's past performance without being compromised by any involvement in its day-to-day operational decisions and activities.

SIRC's research program is designed to address a broad range of subjects. In deciding what to review, SIRC considers:

- events with the potential to create threats to the security of Canada;
- particular activities that could intrude on individual rights and freedoms;
- the CSIS Director's annual classified report to the Minister;
- the need to assess regularly each of the Service's branches and regional offices;
- SIRC's statutory authorities as detailed in the *CSIS Act*;
- priorities and concerns identified by Parliament or in the media;
- commitments by SIRC to re-examine specific matters;
- issues identified in the course of SIRC's complaints functions; and
- new policy directions or initiatives announced by CSIS or the Government of Canada.

This approach allows SIRC to manage the inherent risk of being able to review only a small number of CSIS activities in any given year. Each review results in a "snapshot" of the Service's actions in a particular context. Over more than two decades, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities, and assurance that CSIS is acting lawfully.

SIRC is only one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through the existing apparatus of government, specifically the Minister of Public Safety, the Inspector General of CSIS, the central agencies, the Auditor General, the Information Commissioner and the Privacy Commissioner of Canada.

SIRC REVIEWS IN 2006–07

Review of a security liaison post

Review 2006–01

Background

During the period under review, CSIS maintained a number of Security Liaison Officer (SLO) posts¹ around the world—the number and locations of which are classified, except for those in London, Paris and Washington. These posts work with Citizenship and Immigration Canada to process immigration requests. They also exchange security intelligence information, provide advice to senior staff of the Canadian Mission or Embassy, and liaise with foreign security and intelligence agencies with whom the Service has approved arrangements.

Methodology

SIRC examined how the Service managed its relationships at the post as well as all information exchanges with relevant foreign security and intelligence agencies. SIRC also inquired into the management of CSIS staff at the post, visits to and from the region, and examined the assessments of those agencies with whom the SLO cooperates, a profile of the post itself, and all CSIS studies or reports pertaining to the countries which fall under the post's areas of responsibility. In particular, SIRC evaluated the impact of the immigration security screening workload on other SLO functions.

Findings

SIRC found that the post was managed effectively and that its operations were in accordance with the *CSIS Act*, Ministerial Direction, and operational policy and guidelines. Staff at the post completed and submitted immigration tracking forms on a regular basis, and submitted all required contact and visit forms. The post provided timely and relevant information and advice concerning visits to CSIS Headquarters by foreign representatives. Appropriate approvals were sought and obtained regarding all visits. CSIS's assessments of agencies with which the Service cooperates were, for the most part, completed accurately and submitted in a timely manner, and a new Section 17 arrangement with an organization in the region was established in accordance with Ministerial Direction and operational policy.

¹ SLOs have since been renamed Foreign Officers, as part of a corporate reorganization of CSIS. See Section 2 for details.

All foreign exchanges included the appropriate caveats in accordance with operational policy—specifically, the Service ensured that all information shared with foreign partners was identified as having originated from CSIS, and included restrictions on how it could be used. Finally, SIRC confirmed that the post complied with a CSIS directive not to provide information to or cooperate with a specific foreign intelligence organization during the period under review because of concerns about that agency’s reliability.

There were no recommendations arising from this review.

Review of activities and investigations in a CSIS regional office

Review 2006–02

Background

SIRC regularly reviews, on a rotating basis, the activities and investigations of CSIS in each region of Canada. These regional reviews provide insight into how investigations authorized by CSIS Headquarters are implemented in the field. They also help SIRC gain a better understanding of the priorities and challenges of individual regional offices.

This year, SIRC chose to review CSIS’s smallest regional office, which, despite its size, has full operational and administrative capabilities.

Methodology

For the period September 1, 2004 to August 31, 2005, SIRC assessed the activities of this regional office with reference to the *CSIS Act*, Ministerial Direction and operational policies. SIRC examined the regional office’s:

- targeting approval process and investigation of targets;
- acquisition and execution of warrant powers, along with special operations;
- recruitment, development and tasking of human sources;
- cooperation, liaison and exchanges of information with domestic partners; and
- internal security measures and procedures.

Findings

SIRC found that the operations of the CSIS regional office were in full accord with all applicable laws, directions and policies. CSIS had reasonable grounds to suspect that the targets of authorized investigations in this region posed a threat to the security of Canada, and the intrusiveness of the techniques used was

proportionate to the suspected threat. The information collected by CSIS was strictly necessary to fulfill its mandate. SIRC was pleased to observe that regional staff are responding to emerging threats in a timely and professional manner.

The regional office met all requirements of the Federal Court of Canada in applying for and executing warrant powers in specific investigations. Further, the Service acted appropriately and within the law in its management of human sources. There were a few administrative errors noted in certain human source files, but SIRC considered these minor and they did not affect the Service's investigations.

SIRC found no issues of concern regarding the regional office's cooperation and exchange of information with domestic partners, or with the application of security policies, practices and procedures.

There were no recommendations arising from this review.

Review of a counter-terrorism investigation

Review 2006–03

Background

The focus of this review was a nation-wide CSIS investigation of two Middle East-based organizations listed as terrorist entities under the *Criminal Code of Canada*. The Service's aim was to discover whether there was any formal presence of these terrorist groups in Canada, to identify Canadian-based support networks and to identify persons or groups of persons in Canada who were associated with these Middle Eastern organizations.

Although this was a relatively long-running investigation, there were never more than ten approved targets during the review period of September 1, 2002 to November 30, 2005. By the end of 2005, CSIS had not identified any formal organized presence of these groups in Canada, but the Service had initiated several new investigations of individuals believed to be either linked to, or acting on behalf of the organizations under investigation.

Methodology

This was the first time that SIRC had examined this particular investigation. SIRC analysed documentation pertaining to: the targeting of individuals suspected of engaging in threat-related activities; the management of human sources against authorized targets; and all exchanges of information with domestic and foreign organizations.

Findings

The Service's identification and investigation of targets were found to be in full accord with the *CSIS Act* as well as applicable Ministerial Direction and operational policies. In each investigation, CSIS had reasonable grounds to suspect a threat, and the targeting authorities were proportionate to the seriousness of the threats. CSIS investigators collected only information that was strictly necessary to the investigation.

SIRC noted that the investigation suffered from a lack of resources throughout the review period, and that administrative responsibility for this file shifted repeatedly among CSIS operational desks. This had adverse consequences on the management of information and, to some degree, on the management of human sources. However, generally speaking, SIRC found CSIS to be in compliance with operational policies in the handling of its human sources.

Section 2 of the *CSIS Act* prohibits the investigation of individuals involved in lawful advocacy, protest or dissent (LAPD), unless such activities are carried out in conjunction with threats to the security of Canada. Operational policy therefore requires that investigations which come into contact with LAPD receive special, high-level authorization.

SIRC noted one case where policy requirements were not met. The Service was investigating several members of a Canadian-based community centre because it believed these individuals were engaged in threat-related activities unrelated to the centre's LAPD endeavours. SIRC's review confirmed that the Service's investigation was not focussed on these LAPD activities. Nonetheless, operational policy requires senior-level authorization because of the individuals' involvement in LAPD activities. SIRC found that CSIS investigators failed to obtain the appropriate senior-level authorization in this case, and reminded the Service of their obligation to do so.

The Service's exchanges of information with domestic and international partners were appropriate, although a difficult working relationship with one foreign agency did affect CSIS's investigations during the review period. SIRC also saw one case where ineffective coordination between CSIS and the RCMP resulted in CSIS losing track of an individual for several months. The RCMP and CSIS had exchanged information irregularly on this person. As a consequence of the RCMP's decision to downgrade its investigation, CSIS no longer had accurate information regarding the individual's whereabouts. CSIS could not locate the individual in the ensuing five months, until it learned that the individual was no longer in the country, whereupon CSIS terminated its investigation.

Finally, SIRC reviewed a case of a Canadian citizen detained by a foreign country for suspected involvement in terrorist activity. Media reports alleged that the individual had been mistreated while in detention. SIRC concluded that the Service had conducted an effective and appropriate investigation of the terrorism allegations and of the alleged mistreatment of the detainee. It also found that CSIS upheld its responsibility to the Department of Foreign Affairs and International Trade (DFAIT)—the lead agency responsible for this case.

There were no recommendations arising from this review.

Review of a Section 16 activity

Review 2006–04

Background

Under the provisions of Section 16 of the *CSIS Act*, either the Minister of National Defence or the Minister of Foreign Affairs may request, in writing, the assistance of the Service in collecting foreign intelligence within Canada. Foreign intelligence is defined as information or intelligence relating to the capabilities, intentions or activities of any foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.

If the Minister of Public Safety agrees with the request, it is passed to the Director of the Service, along with written concurrence and direction. CSIS may retain in its Section 12 database any foreign intelligence it collects only if it aids investigations falling under Section 12 of the *CSIS Act*.

The *Act* specifically prohibits any Section 16 collection being directed at Canadian citizens, landed immigrants or Canadian corporations. In the event that CSIS chooses not to retain Section 16 information for a Section 12 investigation, SIRC's jurisdiction ends once the material has been provided to the requesting minister.

A 1987 Tri-Ministerial Agreement establishes the roles and responsibilities of all parties involved in Section 16 collection. One such party is the Communications Security Establishment (CSE), which provides technical assistance in the collection of foreign intelligence.

Section 16 information which CSE provides to the Service is routinely “minimized” to comply with various directions governing the prohibition against targeting Canadian nationals and Canadian businesses. Thus, the name of a Canadian person or entity, collected incidentally, would be reported to the Service

using language such as “a Canadian person” or “a Canadian company.” Under specific circumstances defined in policy, the Service may request identification from CSE if it can demonstrate that the information relates to activities that could constitute a threat to the security of Canada as defined in Section 2 of the *CSIS Act*.

Methodology

SIRC examined CSIS Section 16 collection on a foreign country (“Country A”)—assessing that activity against the *CSIS Act*, Ministerial Direction and, in particular, the 1987 Tri-Ministerial Agreement. Specifically, SIRC reviewed the following:

- all Section 16 reporting to and feedback from DFAIT in 2005;
- the application for and use of Section 16 warrant powers and handling of associated documents;
- the management of human sources who provided both threat-related information and foreign intelligence; and
- the authorization for a corresponding investigation of threat-related activities, as well as all exchanges of information with DFAIT based on this threat.

SIRC staff also received a briefing from CSIS and spoke informally to other Service employees.

Findings

CSIS’s foreign intelligence collection against Country A met the requirements of the *CSIS Act*, in that it did not involve any targeting of Canadians or Canadian organizations. The application for and use of Section 16 warrant powers, and the management of the human sources reviewed, were also appropriate and in accordance with legal and policy requirements.

The *CSIS Act* restricts Section 16 collection to “within Canada.” This means that CSIS cannot task human sources to collect Section 16 information abroad. Although some sources undertook travel abroad, CSIS did not task these human sources to collect Section 16 information while they were outside of Canada. CSIS did, however, have the authority to task these human sources to collect information abroad under a Section 12 investigation of the threat-related activities of Country A. Some of that information proved to be valuable in meeting DFAIT’s Section 16 requirements.

There were no recommendations arising from this review.

Review of a counter-terrorism investigation

Review 2006–05

Background

Known for its support of al Qaida, this foreign-based group was among the first to be placed on Canada's List of Terrorist Entities. This was SIRC's first review of a Service investigation into suspected threat-related activity in Canada by this foreign-based group. It afforded SIRC the opportunity to look into a particular investigative technique occasionally employed by CSIS.

Methodology

SIRC reviewed the Service's investigation from January 1, 2003 to December 31, 2005. The objective of this review was to gain an understanding of this investigation and its challenges, and to assess the Service's compliance with the *CSIS Act*, Ministerial Direction and operational policies.

Specifically, SIRC reviewed the:

- investigation and the targeting approvals of suspected group members;
- implementation and execution of Federal Court warrant powers against the principal targets;
- management of human sources, including those under development;
- advice to government and domestic exchanges of information; and
- exchanges of information and cooperation with foreign intelligence agencies.

In addition, SIRC received two briefings—an overview of the Service's investigation, plus a meeting with the lead CSIS investigator to discuss the Service's interaction with the principal targets.

Findings

Overall, SIRC found that the Service complied with the *CSIS Act*, as well as Ministerial Direction and operational policies in its investigation of the targets. The information collected by CSIS did not indicate that the group's members were involved in terrorist activities while in Canada, and CSIS therefore concluded that they were not an active, operational terrorist cell within Canada. SIRC agreed with CSIS's assessment that it had reasonable grounds to suspect that the activities of the principal targets posed a potential threat to the security of Canada.

There were no recommendations arising from this review.

Review of CSIS's collaboration and exchanges of intelligence post-9/11

Review 2006–06

Background

This review was prompted in part by changes in CSIS's relationships with foreign and domestic partners post-9/11. CSIS is exchanging greater amounts of information with its foreign partners, and with a greater number of foreign partners than in the past. Domestically, the RCMP's role in investigating security threats has grown following the passage of the *Anti-Terrorism Act*, which criminalized actions affecting the national security of Canada. As a result, there is increasing pressure on CSIS to provide support for RCMP prosecutions.

Methodology

This review examined CSIS's relationship with one of its foreign partners and with the RCMP. The objective was to assess compliance with the *CSIS Act*, Ministerial Direction, Memoranda of Understanding (MOU) and operational policies, and to review generally CSIS's performance in the context of its relationship with the RCMP.

To that end, SIRC examined all exchanges of information with the RCMP, all files pertaining to the CSIS-RCMP relationship at headquarters and in two regional offices, and all documents pertaining to CSIS's relationship with two Integrated National Security Enforcement Teams for the 2005 calendar year.² SIRC also examined CSIS's targeting of two individuals between January 1 and July 31, 2005.

Concerning the foreign agency, SIRC reviewed all exchanges of information between 2001 and 2005, CSIS's 2001 and 2006 assessments of the agency, and all files pertaining to its relationship with the agency for the 2005 calendar year.

² More information on the Integrated National Security Enforcement Teams program is available in Section 2 of SIRC's 2002–03 Annual Report.

Findings

CSIS's exchanges of information with the foreign agency were within the scope of the foreign arrangement and complied with the *CSIS Act*, Ministerial Direction and relevant operational policies. SIRC had some concerns about internal mis-communication, as some CSIS officers did not know the status of CSIS's relationship with the foreign agency during the 2002–04 period. This resulted in the SLO receiving incorrect tasking. There was, however, no improper exchange of information.

CSIS's exchanges of information with the RCMP were authorized under the *CSIS Act* and in accordance with Ministerial Direction and relevant operational policies. Looking more generally at the CSIS-RCMP relationship, SIRC noted a spirit of goodwill between the two organizations, as reflected in the new MOU—signed on September 12, 2006—and other initiatives. This new MOU replaces the original one signed in 1990, which had become obsolete.

However, certain challenges remain. SIRC identified two instances that appeared to cause significant friction between CSIS and the RCMP in 2005. The first was an attempted RCMP prosecution using CSIS information. The second concerned the activities of a CSIS human source, which complicated an RCMP investigation for the purposes of criminal prosecution. SIRC notes, however, that there have been positive developments in the CSIS-RCMP relationship in that region since 2005.

SIRC has already noted that the mechanism for exchanging information—in particular, the requirement that the RCMP seek and receive CSIS's explicit permission before using CSIS information in judicial proceedings—was “brought into question”³ by the 1991 Supreme Court decision, *R. v. Stinchcombe*, requiring the Crown to disclose all relevant information to defence counsel. In 2007, CSIS and the RCMP established a working group to review and improve the process for using security intelligence in criminal prosecutions of national security offences.

There were no recommendations arising from this review.

³ Report 101, CSIS Cooperation with the Royal Canadian Mounted Police, Part 1 as reported in Section 1 of SIRC's 1997–98 Annual Report.

Review of security screening outside of the federal government

Review 2006–07

Section 13 of the *CSIS Act* enables the Service to provide security assessments to federal and provincial governments, as well as police forces and foreign entities. The goal of the Security Screening program is twofold: to prevent a non-Canadian who poses a security concern or risk from entering or receiving status in Canada, and to prevent anyone of security concern from gaining authorized access to sensitive government assets, locations or information.⁴

CSIS security assessments fall into two main program categories:

1. Immigration, whereby the Service provides security assessments to Citizenship and Immigration Canada and the Canada Border Services Agency to support the processing of refugee claims or applications for immigration or citizenship; and
2. Government Security Screening, whereby the Service:
 - provides security assessments to all federal departments and institutions, with the exception of the RCMP;
 - complies with requests from foreign agencies (via arrangements with other countries) concerning Canadians who are candidates for employment in a foreign country and require access to classified material; and
 - provides security assessments for non-clearance related programs such as: nuclear sites, the Parliamentary Precinct, provincial governments, sites of interest in respect to national security (e.g., airports and ports) and other programs.

It should be noted that some programs fall under the Government Security Policy while others, such as the Airport Restricted Access Clearance Program and the Free and Secure Trade program, are performed under different authorities and thresholds.

This review focused on assessments for non-clearance related programs.

⁴ For more information on CSIS's Security Screening activities, please see Section 2 of this Annual Report.

Methodology

SIRC assessed CSIS's compliance with the *CSIS Act*, Ministerial Direction, operational policies, the Government Security Policy and relevant Memoranda of Understanding between the Service and its clients. SIRC conducted an in-depth review of a six-month sample of cases and a detailed analysis of all Information Briefs⁵ issued during the review period (there were no denial briefs issued during the review period of April 1, 2004 to March 31, 2006).

Findings

SIRC found considerable variance in the uniformity of Information Briefs, and a lack of consistency in the recording and transcribing of interviews conducted for use within these briefs.⁶ SIRC was pleased to note that the Service only conducted screening checks for foreign agencies where an approved arrangement was in place, and that no recommendations were made, as per policy, to foreign entities. Finally, the Service complied with Ministerial Direction in keeping security screening information segregated from the Service's other information holdings because of its sensitivity for the individuals undergoing assessment.

Recommendations

SIRC made two recommendations arising from this review:

- SIRC observed a lack of differentiation in Information Briefs between varying degrees of risk posed by security screening subjects. For example, the Service assessments of a subject's links with individuals known or thought to be threats to national security were supported in some cases by what SIRC considered to be less compelling information than in others. In another example, although some security screening subjects were offered the opportunity to address security issues in an interview with Security Screening Branch, others were not. SIRC found it problematic that no gradation exists within Information Briefs to address varying degrees of risk of screening applicants, and that these briefs were neither uniform nor consistent as required by policy. SIRC consequently recommended that the Service create policy to address this issue.
- SIRC noted that midway through the review period, the Service abandoned the practice of retaining written consent forms for security assessments conducted for a foreign agency, making it impossible to determine that consent had, in fact, been sought and obtained. SIRC recommended that in cases where the Service

⁵ Information Briefs are issued by CSIS in government screening cases when CSIS uncovers information which may be of concern. They are provided to the requesting agency which then decides whether or not to grant an applicant a security clearance or site access.

⁶ The Service has since changed the policy dealing with interviews.

cannot access written consent forms after the fact (i.e., foreign agencies), these forms be obtained for all security assessments.

Review 2006–08

Note:

Review 2006–08 had not been finalized at the time this annual report went to print. A summary of this review will appear in SIRC's 2007–08 annual report.

Review of the CSIS Counter Espionage Investigations desk

Review 2006–09

Background

Since 9/11, western intelligence agencies have increasingly shifted their attention and resources to counter-terrorism investigations. But there remain other security threats that need to be addressed. In 2006, CSIS and other federal authorities were involved in the arrest and deportation of a Russian spy who had been living in Canada for several years under a false identity. The case serves as a reminder that Canada remains a target of foreign espionage.

This was acknowledged by CSIS Director Jim Judd in an October 2006 address to the annual Canadian Association for Security and Intelligence Studies conference. He noted that “foreign espionage is, if anything, growing and in fact becoming even more sophisticated through the application of new technologies.”

One of the ways the Service combats this threat is through its Counter Espionage Investigations desk. It was formed in 2002 to compartmentalize sensitive counter-espionage investigations which could lead to the prosecution of individuals who knowingly provide sensitive information or assets to hostile intelligence services or foreign governments in a manner detrimental to Canadian interests.

Methodology

SIRC's review examined the activities carried out by the Counter Espionage Investigations desk to assess compliance with the *CSIS Act*, Ministerial Direction and operational policies. It also explored how the Service investigates and supports the prosecution of counter-espionage offences through information sharing with law enforcement agencies.

SIRC chose two investigations for in-depth review. For each, SIRC examined targeting decisions, investigative activities, operational reporting, as well as cooperation and exchanges of information with domestic and foreign partners. Because of the sensitivity of these cases, SIRC is prevented from offering any further details in this report.

Findings

SIRC found that CSIS complied with the *CSIS Act*, Ministerial Direction and operational policies in carrying out counter-espionage investigations.

In the first investigation, SIRC found that close cooperation between CSIS and its domestic and foreign counterparts allowed a "serious security issue" to be resolved in a timely and efficient manner.

In the second investigation, SIRC found that CSIS's disclosure of information allowed the RCMP to take action against an individual engaged in unlawful activities.

There were no recommendations arising from this review.

B. Section 54 Report

Section 54 of the *CSIS Act* entitles SIRC to provide the Minister of Public Safety with a special report on any matter relating to the performance of CSIS's duties and functions. SIRC determined that the events involving Mohammed Mansour Jabarah, as well as concerns raised by the Canadian Civil Liberties Association, were of sufficient importance to warrant a report of this nature.

In April 2005, the then-Minister of Public Safety wrote to the Canadian Civil Liberties Association to assure them that CSIS's actions in this investigation were "appropriate and in accordance with its mandate." The Committee does not know on what advice the Minister based her response, but SIRC's analysis suggests that Section 12 of the *CSIS Act* would not have authorized all aspects of the investigation. This serves as a reminder of the importance of Ministers receiving accurate and comprehensive advice on such sensitive matters.

Review of the case of Mohammed Mansour Jabarah

Review 2005-05

Background

Mohammed Mansour Jabarah, a Canadian citizen, is an admitted al Qaida member and leader of a terrorist cell that planned to bomb the American and Israeli embassies in Singapore and Manila. If successful, the result could have been catastrophic. However, when the plan was thwarted he fled and was apprehended in Oman in March 2002. On short notice, CSIS officials travelled to Oman and unexpectedly found themselves having to arrange for Jabarah to return to Canada. CSIS paid for his ticket.

This investigation was unusual, if not unique, on several levels. In the post-9/11 environment, Canada was working hard to learn as much as possible about the threat from al Qaida, and to demonstrate its reliability as a close ally of the United States in the fight against terrorism.

Nevertheless, despite Jabarah's admissions, he could not be charged under the *Criminal Code*, since all of his terrorist activities pre-dated Canada's *Anti-Terrorism Act*. CSIS engaged in consultations with Jabarah which led him to sign an agreement to facilitate his entry into the U.S. In May 2002, he was transported there with the assistance of CSIS and subsequently pleaded guilty to a number of terrorism-related offences. At the time SIRC's review was finalized, Jabarah had still not been sentenced and he remains incarcerated.

SIRC decided to name this individual in its Annual Report, given that so much information about this case is already in the public domain. On August 14, 2007, the Privacy Commissioner was informed of SIRC's decision. This was done under paragraph 8(2)(m) of the *Privacy Act* which permits the disclosure of personal information when "the public interest in the disclosure clearly outweighs any invasion of privacy."

Methodology

SIRC reviewed this investigation against CSIS operational policy and procedures, Ministerial Direction and applicable Canadian law, including the *CSIS Act* and the *Charter of Rights and Freedoms*. SIRC was also mindful of two facts: that Jabarah is a Canadian citizen, and that Canadian officials must act in accordance with the law.

SIRC examined classified, electronic and hard copy documentation concerning: CSIS's role during Jabarah's time in Oman and during his accompanied travel from Oman to Canada; after his return to Canada; and his transfer to American custody. The Committee also reviewed unclassified, open source material (a book, letters, media reports, etc.). In addition, SIRC received a general briefing from CSIS and an extensive briefing from the investigators assigned to this case. SIRC also obtained legal advice from the Honourable Gérard LaForest, C.C., Q.C., a former member of the Supreme Court of Canada who is a recognized expert on the *Charter*.

Because of the nature and gravity of the issues raised by its review, the Committee decided to submit its findings and recommendations directly to the Minister of Public Safety, under Section 54 of the *CSIS Act*.

Findings

This review highlights a much wider debate occurring in most western democracies. In a November 2004 speech, Mr. Justice Ian Binnie of the Supreme Court of Canada characterized the competing demands of national security and human rights as a “clash of titans.”

In reviewing this case, SIRC acknowledges that the context for these events, soon after 9/11, was such that the protection of Canada and cooperation with Canada’s close allies were priorities across the security and intelligence community. SIRC was also told that CSIS believed that Jabarah had consented freely and voluntarily to cooperate with CSIS and to relinquish his liberty to a foreign jurisdiction.

Nevertheless, the Committee approached this study with the knowledge that Section 32 of the *Charter* applies to the actions of CSIS. Ministerial Direction further reinforces the requirement for CSIS to comply with the *Charter*. Because of events that occurred while Jabarah was in Canada and because CSIS helped to arrange his transportation to the U.S. on a Canadian government-owned aircraft, SIRC sought assurance that CSIS had exercised due diligence to ensure its actions were in accordance with Canadian law.

SIRC’s review raised questions regarding CSIS’s contention that Jabarah’s decisions were made freely and voluntarily. SIRC concurs with LaForest that several of the circumstances surrounding this case would lead a court to scrutinize meticulously the actions of CSIS officials to determine whether Jabarah’s decisions were completely voluntary. His decisions—made without the benefit of any independent legal advice—resulted in Jabarah’s self-incrimination and surrender to U.S. authorities. SIRC believes a court would also have considered other factors, including: his age; his emotional state; whether his fear of the alternatives influenced his return to Canada from Oman; the length of time he spent in the company of CSIS officials while in Canada; and the circumstances surrounding his decision to surrender himself to a foreign jurisdiction.

SIRC was told by a CSIS investigator that Jabarah was not “read his rights” because CSIS is not a police service. This response—subsequently confirmed in writing by the Service—demonstrates a misunderstanding of the application of the *Charter* to government representatives carrying out their official duties.

Jabarah could not be prosecuted for any crime in Canada, since his terrorist activities pre-dated Canada's *Anti-Terrorism Act*. Neither CSIS nor the police had any right to detain him. Based on these and other circumstances, the Committee concluded that Jabarah was "arbitrarily detained" by CSIS in violation of Section 9 of the *Charter*. Because he was detained, his right to silence as protected by Sections 7 and 11(c) was violated, as was his right to counsel under Section 10. Furthermore, his right to remain in Canada as protected by Section 6 of the *Charter* (mobility rights) was breached.

Another Canadian agency informed CSIS that Jabarah could not be criminally charged, since the acts which he committed did not take place in Canada and were not crimes in Canada at that time. However, CSIS knew that Jabarah could be prosecuted in the U.S. During its review, SIRC became aware of actions undertaken by CSIS (which remain classified) that materially assisted U.S. law enforcement officials. For that reason, SIRC believes that CSIS could not be independent with respect to any consultations that it carried out with Jabarah. Moreover, these actions led SIRC to conclude that CSIS strayed from its security intelligence mandate into the area of law enforcement.

Finally, SIRC found that it was missing some documentation relevant to its review. SIRC saw references to meetings for which minutes were not kept, to interdepartmental consultations for which there were no written records, and to operational email messages that had been deleted. SIRC was concerned by these gaps in the written record. It was especially troubled that an investigation of such importance and sensitivity—which had a direct impact on the indictment and prosecution of a Canadian by U.S. authorities—could be conducted by CSIS without requesting any formal legal advice from the Department of Justice.

Recommendations

SIRC made six recommendations stemming from this review:

- The 1987 Memorandum of Understanding (MOU) between CSIS and the Department of Foreign Affairs and International Trade (DFAIT) be updated to designate Foreign Affairs as the lead agency in cases involving Canadian citizens detained abroad. The MOU should also reflect the protocol recommended by Mr. Justice O'Connor, namely, "timely and open consultation among Canadian agencies" involved with Canadians detained abroad, "a coherent and unified approach" led by DFAIT and "accountability for the course of action adopted" in such cases.

- CSIS amend its policies so that emails are automatically retained unless there is a conscious decision to delete them.
- The Service clearly communicate to its employees what would constitute “recorded information,” as distinct from “transitory records,” and should therefore be filed and retained under applicable federal legislation.
- Whenever possible, CSIS keep written records of its interdepartmental consultations, including but not limited to its formal and informal consultations with DFAIT and the Department of Justice.
- CSIS ensure that the storage, retention and retrieval of all operational information under its control, including email messages, is in accordance with applicable federal legislation, including the *CSIS*, *Privacy*, *Access to Information* and *Library and Archives of Canada Acts*.
- CSIS request and obtain written advice from the Department of Justice in operations where an individual is questioned in circumstances which may give rise to a detention, in order to ensure that the individual’s *Charter* rights are respected, and in all occasions when it is unclear whether the Service’s activity falls within its statutory mandate under Section 12 of the *CSIS Act*.

Conclusion

Jabarah is a terrorist but also a Canadian citizen, and no matter how despicable his actions, the *Charter* conferred on him certain fundamental rights. SIRC’s mission is to protect Canadians’ rights by ensuring that CSIS acts within the law. Therefore, the Service must comply with the *Charter* in carrying out its investigations as mandated by the *CSIS Act*, no matter what unexpected circumstances may arise.

C. Investigation of complaints

HOW SIRC INVESTIGATES COMPLAINTS

In addition to its review function, SIRC is responsible for investigating complaints about CSIS. Almost all complaint cases begin as inquiries to SIRC—either in writing, in person or by phone. SIRC staff respond promptly to such inquiries, usually instructing the prospective complainant about what the *CSIS Act* requires for a concern to become a formal complaint.

Once a written complaint is received, SIRC conducts an initial review. Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated. If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee members, assisted by staff.

In investigating complaints, SIRC has all of the powers of a superior court, and has access to all information in the possession of CSIS, except for Cabinet confidences.

A complainant has the right to be represented by counsel and to make representations at the hearing. Pre-hearings may be conducted to establish and agree on procedures with the complainant and/or the complainant's counsel. SIRC's Senior Counsel provides legal advice on procedural and substantive matters, and will also cross-examine Service witnesses when, for national security reasons, evidence must be heard without the complainant being present.

Types of complaints

Four kinds of matters may be investigated by SIRC:

- Complaints lodged by persons “with respect to any act or thing done by the Service” (Section 41);
- Complaints concerning denials of security clearances to government employees or contractors (Section 42);
- Referrals from the Canadian Human Rights Commission of allegations made to it; and
- Minister's reports in regards to the *Citizenship Act*.

The types of complaints that SIRC investigates are described in the *CSIS Act* and take several forms.

Under Section 41 of the *CSIS Act*, SIRC can investigate “any act or thing” done by the Service. Under Section 42, it can hear complaints about denials of security clearances to federal government employees and contractors. Section 42 does not permit SIRC to accept jurisdiction to hear complaints concerning less intrusive background screening or reliability checks, which are conducted simply to determine the trustworthiness or suitability of a potential federal employee. These complaints are addressed through an organization’s designated grievance procedure.

Pursuant to Section 42 of the *CSIS Act*, individuals who have been denied a security clearance must be informed of this action by the Deputy Head of the organization. These individuals have the right to make a complaint to SIRC, and where appropriate, it will investigate and report its findings and any recommendations to the Minister, the Director of CSIS, the Deputy Head concerned and the complainant.

Should the Canadian Human Rights Commission receive a written notice from a Minister of the Crown about a complaint that relates to the security of Canada, the Commission may refer the matter to SIRC. Upon receipt of such a referral, SIRC carries out an investigation and reports its findings to the Commission, the Director of CSIS, the Minister of Public Safety, the Minister of the department concerned and the complainant. SIRC also has the authority to conduct investigations into matters referred to SIRC pursuant to the *Citizenship Act*.

When SIRC’s investigation of a complaint made under Section 41 is concluded, it provides the Director of CSIS, the Minister of Public Safety and the complainant with a report of its findings and recommendations.⁷ Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC’s annual report to Parliament.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC’s jurisdiction or investigated and resolved without a hearing (i.e., administrative review).

⁷ The complainant receives a declassified version of the report.

Table 1
Resolution of complaints

	2004–2005	2005–2006	2006–2007
Carried over	16	18	24
New	30	45	37
Total	46	63	61
Closed	28	39	41
Carried forward to subsequent year	18	24	20
Reports issued	3	4	5

How SIRC determines jurisdiction of a complaint...

...under Section 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by “any person” with respect to “any act or thing done by the Service.” Before SIRC investigates, two conditions must be met:

1. The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act*.

...under Section 42

With respect to security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

1. Any person refused federal employment because of the denial of a security clearance;
2. Any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
3. Anyone refused a contract to supply goods or services to the government for the same reason.

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

D. SIRC complaint decisions 2006–07

The following are summaries of the five reports issued by SIRC during the period under review, in response to complaints filed.

Alleged discrimination in an immigration process

Report 2006–01

SIRC reported a decision concerning a complaint that was referred to SIRC by the Canadian Human Rights Commission under Section 45 of the *Canadian Human Rights Act (CHRA)*. The complainant in the case alleged discrimination in contravention of the *CHRA* after being denied a “security clearance”.⁸ Since this security assessment was required for the complainant’s immigration process, the allegation was that the complainant was prevented from becoming a Canadian citizen because of the denial of the clearance.

The complaint specifically alleged: a delay by CSIS in processing the complainant’s security assessment which formed the basis of the advice to the Minister of Citizenship and Immigration provided under Section 14 of the *CSIS Act*; accusations made against the complainant by CSIS during an interview with the complainant; and poor treatment by the Service during an administered polygraph examination.

SIRC concluded there was no evidence to support the allegations concerning the Service’s delay in processing the security assessment, or in the manner in which the citizenship interview and polygraph examination were conducted. SIRC found that the Service did not proceed with its investigation with intent to treat the complainant adversely because of his national or ethnic origin. Rather the Service investigated security concerns associated with the complainant’s application for Canadian citizenship.

Recommendation

- SIRC recommended that the Canadian Human Rights Commission not investigate this complaint.

⁸ The original complaint used the term “security clearance.” It should be noted that CSIS provides security assessments which form the basis of a clearance issued by the Minister of Citizenship and Immigration. CSIS itself does not issue clearances in these cases. For more information on the security screening process, see Section 2 of this Annual Report.

Alleged actions by CSIS during a citizenship interview

Report 2006–02

SIRC reported a decision concerning a complaint pursuant to Section 41 of the *CSIS Act* dealing with the alleged actions of CSIS during a citizenship interview.

SIRC found that CSIS failed to provide the complainant with proper notice before it conducted the citizenship interview. SIRC found that although CSIS's report to Citizenship and Immigration Canada contained some errors, the report adequately reflected the content of the complainant's citizenship interview.

Recommendation

- SIRC recommended that CSIS implement a procedure to verify that individuals about to be interviewed by CSIS for citizenship or immigration interviews be given adequate written notice by Citizenship and Immigration Canada that CSIS intends to interview them.⁹

Revocation of a security clearance

Report 2006–03

SIRC reported a decision on a complaint pursuant to Section 42 of the *CSIS Act*, concerning the revocation of a security clearance of a CSIS employee, which ultimately led to the employee's dismissal.

The complainant held a Top Secret security clearance. According to the Government Security Policy, a Top Secret security clearance may not be granted where there are reasonable grounds to doubt the applicant's loyalty to Canada or reliability as it relates to loyalty.

SIRC concluded there were reasonable grounds to believe the complainant:

- May have knowingly associated with individuals considered to be a security threat;
- Failed to report to CSIS self-admitted suspicions about those individuals' activities; and

⁹ SIRC has since been informed by CSIS that CIC is now notifying immigration interviewees about whether or not their interview will be conducted by the Service.

- May have disclosed classified information, which was a breach of security.

SIRC concluded the Director had reasonable grounds to revoke the complainant's security clearance.

Recommendations

SIRC recommended that CSIS:

- Create and implement a policy requiring that its employees be informed of their right to legal representation and be given an opportunity to consult with a legal representative before and while an interview is conducted for the purposes of either a breach of security or a breach of conduct investigation;
- Create a roster of lawyers from the private sector who have a Top Secret clearance whom CSIS employees may retain;
- Create and implement a policy by which its investigators must declare a conflict of interest when an individual seeks their opinion about the retention of legal counsel;
- Create and implement a policy requiring that its employees input relevant information in a timely manner;
- Amend its policy dealing with the destruction of investigative materials—including audio cassettes and notes—concerning a breach of security investigation or a disciplinary investigation;
- Remind its employees that SIRC has the statutory right to access all information under the control of CSIS—except for matters of Cabinet confidence—including audio cassettes, handwritten notes and email messages, and that care should be taken to not destroy information that could have an impact on SIRC's ability to exercise its right to access such information; and
- Place greater emphasis on employees' obligations with respect to the protection of classified information in its orientation course and other security briefings.

Alleged false statements

Report 2006–04

SIRC reported a decision on a complaint made pursuant to Section 41 of the *CSIS Act* by Human Concern International (HCI), alleging that the Service made a false statement to the Federal Court of Canada, via the Minister of Public Safety and the Minister of Citizenship and Immigration. It was further alleged that a document filed by both Ministers was based on CSIS information that the Service knew—or ought to have known—would impugn the character, reputation and

standing of the complainant. Furthermore, HCI maintained that not being party to the court proceedings meant there was no formal opportunity to challenge a statement by the Service that was later published in two Canadian newspapers.

Upon receipt of this complaint, SIRC encouraged the two parties to seek an alternative resolution of this dispute. When these discussions failed, SIRC undertook its own investigation. It found that the Service had made an unsubstantiated allegation about the complainant in its advice to the Ministers of Public Safety and Citizenship and Immigration which was in turn presented to the Federal Court. As well, SIRC found that CSIS knew that reliance would be placed on its advice by both the Ministers of Public Safety and Citizenship and Immigration, as well as the Federal Court. For this reason, and since HCI was not given an opportunity to respond to the impugned statement, CSIS should have taken care to avoid making an unsubstantiated statement which could lead to injury or loss of support and funding.

Recommendations

SIRC recommended that:

- CSIS formally retract this particular statement and that it do so by informing the Minister of Citizenship and Immigration, the Minister of Public Safety, the Federal Court of Canada and the publishers of two newspapers; and
- CSIS apologize to HCI for having made an unsubstantiated statement.

Alleged delay in processing a citizenship application

Report 2006–05

SIRC reported on another complaint made pursuant to Section 41 of the *CSIS Act*, which alleged that CSIS deliberately and improperly caused a delay in the processing of the complainant's citizenship application. The complainant, a permanent resident of Canada, applied for Canadian citizenship and was the subject of a security screening interview conducted by the Service, as requested by Citizenship and Immigration Canada (CIC).¹⁰

¹⁰ Section 14 of the *CSIS Act* allows the Service to advise any Minister of the Crown on matters relating to the security of Canada, or provide any Minister of the Crown with information relating to security matters or criminal activities.

In this case, CSIS explained to SIRC that the investigator's delay in filing the report of the interview with the complainant had occurred partly due to workload issues in the aftermath of 9/11.

SIRC's authority under Section 41 of the *CSIS Act* does not extend to investigating CIC. Therefore, it was unable to determine CIC's role in any delay in the processing of the complainant's citizenship application. Regarding the Service's role, SIRC found that the Service:

- delayed in scheduling the interview between the complainant and the screening investigator;
- delayed in completing and filing the interview report; and
- contributed to additional delays by recommending that CIC consult with another federal agency.

SIRC determined, however, that these delays—although regrettable—were unforeseeable and found the complainant's allegations were unsupported.

Section 2

CSIS accountability mechanisms

CSIS accountability mechanisms

A. Reporting requirements

CSIS DIRECTOR'S ANNUAL REPORT (2005–06)

Each year, the Director of CSIS must submit a classified report to the Minister of Public Safety, detailing the Service's priorities and operational activities. The *CSIS Act* also requires that the Inspector General of CSIS examine this report and submit a certificate to the Minister, which attests to the extent to which she is satisfied with its contents. Finally, the Minister sends a copy of both documents to SIRC for its review, as required by Section 38(a) of the *CSIS Act*.

According to the Director's Annual Report, the central priorities of the Service are the assurance of public safety and safeguarding of key critical infrastructure. The Director noted that he supports appropriate lawful access legislation to enhance CSIS's ability to meet these priorities. He believes such legislation would enhance intelligence-gathering capabilities and facilitate CSIS's access to modern telecommunications networks.

The investigation of terrorism and terrorist threats to Canada and Canadian interests abroad remain the Service's highest operational priority, in particular the numerous threats posed by Islamist extremism. The Director emphasized that the threat from al Qaida was most acute overseas, and that many of the Service's targets (including some Canadian citizens) are involved in international terrorist groups whose activities directly threaten Canadian interests internationally.

The Service continued to expand its role in supporting Canadian forces abroad. In 2005–06, this included support for Canadian forces in Afghanistan, involvement in the mission to recover Canadian hostages in Iraq and assistance in the evacuation of Canadian citizens from Lebanon. The Director publicly acknowledged these activities in October 2006.

In addition, the Director reported that CSIS had ongoing investigations into many domestic terrorist-related activities, including the threat of serious violence related to Native extremism, militant Quebec nationalism and white supremacist and environmental movements. For the second year, the Director emphasized the threat posed by al Qaida inspired, homegrown extremists within Canada such as the ongoing criminal proceedings against fifteen individuals living in Toronto.

The Director's report also noted that the Service continued to investigate attempts by foreign countries to conduct espionage, access proprietary technologies and proliferate weapons of mass destruction. Three countries were considered priorities in 2005–06, but many other countries were engaged in similar activities.

The security screening statistics reported by the Director have already been reported in SIRC's 2005–06 annual report. The Director noted that CSIS expanded its security screening responsibilities by signing agreements with two provinces and assumed new obligations under a 2005 tripartite agreement, the Security and Prosperity Partnership of North America.

The Director noted that CSIS expanded its cooperative network with domestic partners by adding two new Memoranda of Understanding in 2005–06. He also reported that CSIS maintains excellent relations with its key foreign partners. Emphasis was also placed on how the Service exercises due diligence concerning the human rights records of partner countries or agencies, and that it continues to provide training to new intelligence services on the principles of intelligence collection in democracies.

Readers should note that CSIS posts public, unclassified reports on its website (www.csis-scrs.gc.ca).

CERTIFICATE OF THE INSPECTOR GENERAL OF CSIS (2006)

The position of Inspector General (IG) was established in 1984 under the *CSIS Act*. The IG carries out internal reviews of CSIS on behalf of the Minister of Public Safety, reviewing the Service's operations and providing assurance that CSIS is complying with the *CSIS Act*, Ministerial Direction and operational policy.

Every year, the IG submits a certificate to the Minister stating the extent to which he or she is satisfied with the CSIS Director's Annual Report. The certificate also informs the Minister of any instances of CSIS failing to comply with either the *Act* or Ministerial Direction, or an unreasonable or unnecessary exercise of its powers.

The IG reported being satisfied with the 2005–06 CSIS Director's Annual Report, but noted there were some discrepancies between the statistics reported and the facts provided to the IG. The IG found that the Service had not acted beyond its statutory authority and that it exercised its duties and functions effectively and professionally.

The IG reported that for 2005–06, there was an increase in the number of incidents of non-compliance with operational policy. The IG defines non-compliance as any action that is not in adherence with rules, procedures, principles and guidelines set out in operational policy. She does not differentiate the relative importance of any instance of non-compliance.

Among the concerns brought forward by the IG was that CSIS's 2005 annual direction statement was based on national security intelligence requirements issued to CSIS by an ad-hoc Cabinet Committee. According to the IG, the national requirements become a Cabinet Confidence and therefore limit the IG's right of access to all CSIS information.

The IG found several cases where information was mishandled, including cases where her staff found discrepancies and inaccuracies in CSIS files, as well as instances where CSIS was unable to locate or retrieve documentation requested.

The IG identified several gaps in current CSIS policy. She noted that the policy framework did not reflect the current procedures for the approval of information exchanges with partner agencies. The IG observed that there is a growing disconnect between policy and practice with respect to the execution of warrant powers.

Section 16 of the *CSIS Act* requires the Service to limit the collection of foreign intelligence to within Canada, while security intelligence collected under Section 12 may be obtained within Canada and abroad.¹¹ In her 2006 certificate, the IG noted considerable overlap between the Service's Section 12 and Section 16 investigations, leading her to conclude that in some cases, the effect of the geographical restriction of Section 16 is meaningless.

Finally the IG concluded that she observed a gap in operational policies governing certain CSIS operations overseas.

For more information, please refer to the Inspector General's home page on the Public Safety website (publicsafety.gc.ca).

¹¹ See SIRC review 2006-04 for details on a Section 16 activity.

UNLAWFUL CONDUCT BY CSIS

Under Section 20(2) of the *CSIS Act*, the Director of CSIS must submit a report to the Minister when, in the Director's opinion, a CSIS employee may have acted unlawfully in performing his or her duties or functions. The Minister, in turn, must send the report with his or her comments to the Attorney General of Canada and to SIRC. In 2006–07, no CSIS employees acted unlawfully, and no such reports were issued.

DISCLOSURES OF INFORMATION

Section 19 of the *CSIS Act* prohibits information obtained by the Service in the course of its investigations from being disclosed except in the following specific circumstances:

1. information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law may be disclosed to a law enforcement agency having jurisdiction over the matter, the Minister of Public Safety or the Attorney General of the province in question;
2. information related to the conduct of Canada's external relations may be disclosed to the Minister of Foreign Affairs;
3. information related to the defence of Canada may be disclosed to the Minister of National Defence; and
4. information that, in the opinion of the Minister, is essential to the public interest may be disclosed to any Minister of the Crown or employee of the Public Service of Canada.

Of note, Section 19(2)(d) gives the Minister of Public Safety the power to override any invasion-of-privacy concerns, authorizing the Service to disclose information deemed to be in the national or public interest. When such information is released, the Director of CSIS must submit a report to SIRC. This is an exceedingly rare occurrence—there have been only two disclosures under this Section of the *Act*.

The Service may also disclose information verbally or in writing to any law enforcement body or federal government entity, such as the Department of National Defence and Foreign Affairs Canada. When CSIS permits the use of its information by the RCMP in judicial proceedings, it must do so in writing.

The Service provided over 130 disclosure letters during fiscal year 2006–07.

B. Foreign and domestic arrangements

Sections 13 and 17 of the *CSIS Act* allow CSIS to enter into arrangements with foreign and domestic organizations or agencies in order to perform its duties and functions. SIRC receives copies of these arrangements as they are initiated, and examines a selection of them every year.

ARRANGEMENTS WITH DOMESTIC AGENCIES

CSIS often collaborates with federal departments and agencies, provincial governments and law enforcement agencies. Since 9/11, more groups have been involved in national security, including police forces and other government partners. This creates a challenge for the Service, as it must cultivate and maintain healthy relationships with both new and existing partners to ensure that information is exchanged efficiently and that joint operations are conducted effectively.

Although many domestic arrangements take the form of a Memorandum of Understanding (MOU), CSIS may collaborate with any domestic agency whether or not an MOU is in place. As of March 31, 2007, CSIS had 35 MOUs with domestic partners: 19 with federal departments or agencies and 16 with provincial and municipal entities.

In September 2006, the Service updated its MOU with the RCMP. The updated MOU reflects new mechanisms of cooperation and consultation between the two organizations. The MOU also outlines the implementation of a national counter-terrorism strategy to facilitate CSIS-RCMP cooperation and coordination. It establishes counter-terrorism threat overview and investigative priorities common to both organizations, as well as developing joint training programs.

ARRANGEMENTS WITH FOREIGN AGENCIES

As of March 31, 2007, CSIS had 271 foreign arrangements with agencies in 147 countries. New foreign arrangements require the approval of the Minister of Public Safety, in consultation with the Minister of Foreign Affairs. Even without such an arrangement, CSIS can still accept unsolicited information from an agency or organization of a foreign country. The Minister approved seven new arrangements in 2006–07, and expanded six existing ones.

On occasion, the Service must alter foreign arrangements—to accommodate a change in the foreign partner¹², to reactivate a dormant relationship, or to place an arrangement into dormancy. Eight arrangements were altered during the year under review. Another eight were restricted.

The Director of CSIS has the discretion to approve the expansion or alteration of a foreign arrangement without Ministerial approval. These remain subject to any Ministerial caveats or instructions that may have been imposed when the initial arrangement was approved.

SIRC reviews all new, enhanced or modified foreign arrangements, as provided under Section 38(a)(iii) of the *CSIS Act*. To do so, it examines whether:

- CSIS foreign arrangements were in accordance with the conditions set out in the *CSIS Act*, Ministerial Direction and operational policy;
- approvals from the Minister of Public Safety and the Director of CSIS were in place when the Service began exchanging information;
- the human rights record of the foreign agency's host country was considered; and
- the most recent arrangement profile met CSIS guidelines.

In 2006–07, SIRC reviewed 19 foreign arrangements with agencies in 14 countries. SIRC found that all foreign arrangements were in accordance with the *CSIS Act*, Ministerial Direction and operational policies.

SIRC also found that the Service had informed itself of the human rights situation in all the countries and agencies in question. Moreover, the Service had proceeded cautiously with exchanges of information involving countries with questionable human rights records.

SIRC also observed an improvement in the timely submission of arrangement profiles. All of the profiles reviewed by SIRC reflected the current security, human rights and political environment of the countries and agencies in question.

¹² These changes can include merging of two agencies into one, or a change in agency name.

C. Policy and governance

NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE

The Minister of Public Safety issues National Requirements for Security Intelligence, which contain general direction from government regarding where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis and advisory responsibilities.

The 2006–08 National Requirements direct the Service to continue to maintain a flexible capability to meet Canada's evolving security intelligence needs by relying on risk management. The Minister notes that today's threat environment is increasingly international and transnational in nature, with many offshore threats to Canada's security requiring foreign investigations. CSIS is therefore directed to continue to investigate threats to Canada's security both within Canada and abroad.

For 2006–08, the Minister has directed CSIS to pursue the following security intelligence priorities:

- Safeguarding against—and advising the government of—the possibility of a terrorist attack occurring in or originating from Canada, or affecting Canadian citizens or assets abroad;
- Continuing to conduct research and analysis in support of the listing of terrorist entities under the *Criminal Code of Canada* and combating terrorist financing;
- Supporting the Government of Canada's efforts in Afghanistan;
- Working closely with other government departments to combat transnational criminal activity;
- Investigating threats to Canada's national security arising from activities of countries that engage in espionage;
- Continuing to identify and investigate countries and groups that have or may attempt to acquire weapons of mass destruction, and advising the government of the threats posed by these activities;
- Supporting the collection of foreign intelligence in Canada to assist the Minister of Foreign Affairs and/or the Minister of National Defence pursuant to Section 16 of the *CSIS Act*;
- Delivering security screening programs to federal departments, agencies and other clients;
- Providing the Government of Canada with intelligence assessments and ensuring that CSIS keeps itself informed of political, social and economic environments from which threats to the security of Canada may emerge; and

- Ensuring CSIS's technical equipment and information systems meet the requirements of its investigations.

MINISTERIAL DIRECTION

Under Section 6(2) of the *CSIS Act*, the Minister of Public Safety may issue written directions governing CSIS's activities and investigations. The last time the Minister issued such direction was in 2001, when a compendium was provided to SIRC. In June 2007, however, SIRC received the latest *National Requirements for Security Intelligence* for 2006–08 (no direction was issued for 2005–06).

CHANGES IN CSIS OPERATIONAL POLICY

CSIS administrative, security, human resources and operational policies embody rules and procedures that govern the range of activities undertaken by the Service. Administrative, security and human resources policies are all internal corporate policies. Operational policies, which describe how CSIS employees should perform their duties, are updated regularly in accordance with government policy, legislative and other changes. They are reviewed by SIRC to ensure that they conform to the *CSIS Act* and Ministerial Direction.

In 2006–07, CSIS revised and/or published over 120 policies. Some revisions were administrative in nature. The remainder were of an operational nature and pertained to, among other things, warrant acquisition and approvals for Section 12 and 16 investigations. Although no new policies were developed as a result of CSIS's organizational realignment, 14 corporate and 77 operational policies were amended (see **CSIS operational activities**).

One of the policy projects the Service undertook in 2006–07 was the Director's "Delegation of Responsibility" project—a review of all operational policies to determine where executive and management responsibilities must be delegated. CSIS informed SIRC that this project is ongoing and that it would share the results upon its completion.

GOVERNOR-IN-COUNCIL REGULATIONS AND APPOINTMENTS

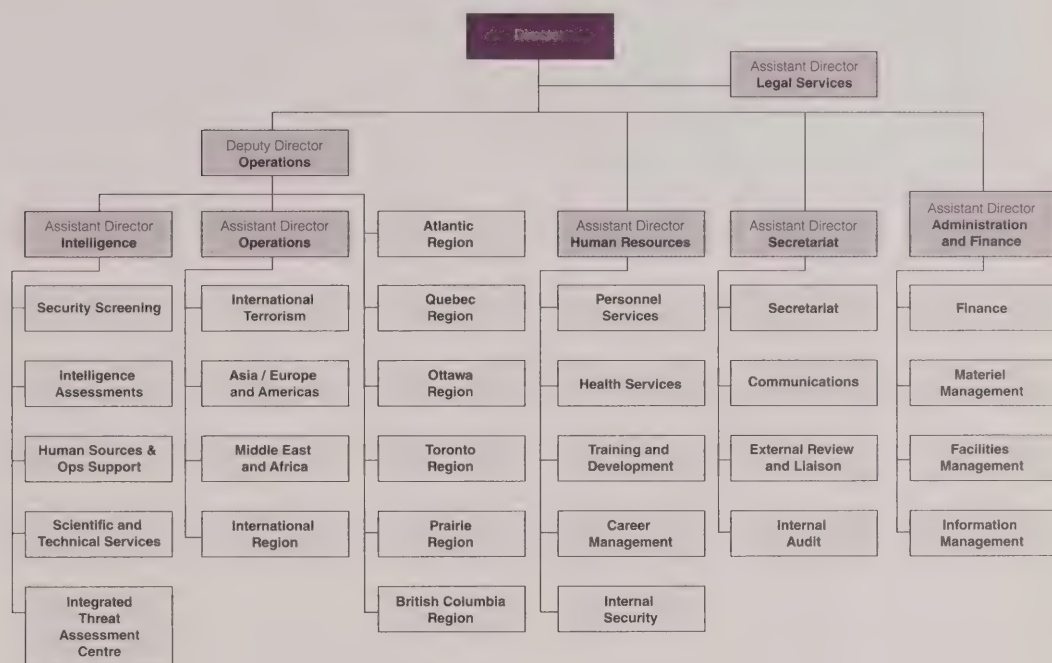
Section 8(4) of the *CSIS Act* states that the Governor-in-Council may issue regulations to the Service concerning the powers and duties of the Director of CSIS, as well as the conduct and discipline of Service employees.

The Governor-in-Council did not issue any regulations in 2006–07.

D. CSIS operational activities

In May 2006, CSIS implemented a new operational structure. According to the Service, this realignment of resources was designed to ensure that CSIS could increase its operational capacity, consolidate and enhance analysis and production facilities and improve corporate support. The Deputy Director Operations, who reports to CSIS's Director, is now responsible for three groups:

Canadian Security Intelligence Service



1. **Intelligence**, consisting of five branches: Security Screening; Intelligence Assessments; Human Sources and Operations Support; Scientific and Technical Services; and the Integrated Threat Assessment Centre;
2. **Operations**, consisting of three branches and one region: International Terrorism; Middle East and Africa; Asia, Europe and Americas; and International Region; and
3. **Six regions.**

The functions of these groups are highlighted below.

1. Intelligence

SECURITY SCREENING BRANCH

One of the largest branches of CSIS, Security Screening has two program streams—government screening and immigration screening.

Government screening performs security clearance investigations for all government employees¹³ whose duties require them to access classified assets or information. The results of these investigations are security assessments—an appraisal of an individual's reliability as it relates to loyalty to Canada—which are provided to the requesting department or agency. Traditionally, the largest clients of this service have been Public Works and Government Services Canada and the Department of National Defence (DND)—accounting for over 28 percent and 26 percent respectively of all requests in 2006–07.

As indicated in Table 2, in 2006–07, CSIS received 51,200 requests for new or updated security clearances and provided 55,000 security assessments to federal departments. The volume of requests increased by approximately 22 percent from the previous fiscal year, and the number of security assessments issued by CSIS increased by 46 percent compared with previous years.

¹³ CSIS does not conduct security clearance investigations on behalf of Canada's national police force. The RCMP conducts these investigations on its own behalf.

Table 2
CSIS government security screening*

	2004-05	2005-06	2006-07
Requests from DND	9,100	9,200	13,100
Requests from other departments or agencies	27,400	32,900	38,100
Total	36,500	42,100	51,200
Assessments issued to DND	9,000	8,900	13,100
Assessments issued to other departments or agencies ¹⁴	27,600	28,900	41,800
Total	36,600	37,800	55,000

* Figures have been rounded to the nearest 100.

To track its efficiency in responding to security screening requests, CSIS calculates its turnaround times using a median number of days. As indicated in Table 3, the median turnaround times increased over the previous year's levels in all but one case. The time it took to process a Level I clearance more than doubled for departments other than DND.

Table 3
Median turnaround time (in calendar days)

		2004-05	2005-06	2006-07
DND	Level I (Confidential)	49	24	40
	Level II (Secret)	63	19	40
	Level III (Top Secret)	70	39	82
Non-DND	Level I (Confidential)	12	15	32
	Level II (Secret)	14	13	21
	Level III (Top Secret)	69	60	47

¹⁴ This number includes assessments performed for provincial governments and for access to nuclear facilities.

The Service does not decide who receives a security clearance. Rather, it advises the requesting department or agency of information that could have an impact on their decision to grant a clearance. On rare occasions, CSIS will recommend to a requesting agency that a clearance be denied. However, it is the responsibility of the requesting agency to accept or reject this recommendation. In 2006–07, the Service issued 14 information briefs reporting information of an adverse nature. No denial briefs were issued.

CSIS also provides site-access screening. Unlike a government security clearance, a site-access clearance only gives an individual access to certain secure areas within buildings or provides accreditation for a special event. In 2006–07, CSIS received over 83,900 requests for this type of screening, and provided three information briefs to requesting agencies. The increase in requests for access to nuclear facilities, which rose by roughly 69 percent, is a result of a five-year renewal cycle for pre-existing clearances.

There were no special events for which the Service provided assessments. All other site-access requests remained close to levels of previous years.

Table 4
Site-access screening*

	2004–05	2005–06	2006–07
Parliamentary precinct	1,100	1,000	1,100
Airport restricted-access area	31,100	37,600	39,300
Nuclear facilities	6,800	10,600	17,900
Canada Border Services Agency (CBSA) / Free and Secure Trade (FAST) ¹⁵	21,500	3,100	23,100
Special events accreditation	1,800	5,600	0
Other government departments	2,300	2,400	2,500
Total	64,600	60,300	83,900

* Figures have been rounded to the nearest 100.

¹⁵ The FAST program came into effect in 2004–05. The data for 2006–07 represents screening requests for both FAST and CBSA, which CSIS is now calculating together.

CSIS advice on security screening can take one of five forms:

1. **Notices of assessment** are issued in those government and immigration screening cases when CSIS finds no adverse information on an applicant.
2. **Incidental letters** are issued to Citizenship and Immigration Canada (CIC) and to the Canada Border Services Agency (CBSA) when the Service has information about an applicant who is or has been involved in non-security related activities described under the *Immigration and Refugee Protection Act (IRPA)*.
3. **Information briefs** are issued in government screening cases when CSIS has information that could have an impact on the requesting agency's decision to grant an applicant a security clearance or site access. It is also provided in immigration screening cases when the Service has information that an applicant is or was involved in activities that do not necessarily warrant inadmissibility for entry into Canada.
4. **Inadmissibility briefs** are issued to CIC/CBSA when an applicant is deemed to be inadmissible to Canada under the security provisions of the *IRPA*.
5. **Denial briefs** are issued when the Service recommends to a requesting agency that a security clearance or site access be denied to an individual.

Immigration screening requires the Security Screening Branch to conduct investigations and to provide advice to Citizenship and Immigration Canada as well as the Canada Border Services Agency to support the processing of refugee claims or applications for immigration or citizenship. The Service's authority in this regard is provided under Section 34(1) of the *Immigration and Refugee Protection Act*.

In 2006–07, the branch received 92,300 requests under various immigration screening programs (see Table 5). The number of requests received within and from outside Canada and the number of refugee determination and front-end screening requests were almost the same as the previous year.

Table 5
Immigration security screening

	Requests*			Briefs		
	2004–05	2005–06	2006–07	2004–05	2005–06	2006–07
Within and outside Canada ¹⁶	56,100	63,200	62,800	88	133	201
Front-end Screening ¹⁷	22,900	17,100	17,900	184	89	143
Refugee determination ¹⁸	14,200	11,700	11,600	110	127	153
Subtotal	93,200	92,000	92,300	382	349	497
Citizenship applications	161,200	308,000	227,300	124	120	155
Total	254,400	400,000	319,600	506	469	652

* Figures have been rounded to the nearest 100.

CSIS finds no adverse information in the vast majority of its screening investigations of refugee claimants or immigration/citizenship candidates. In 2006–07 the Service issued 157 information briefs, 44 inadmissibility briefs and 2 incidental letters related to immigration cases.

As has been the case in recent years, the Service's turnaround times for providing information or inadmissibility briefs were generally quite lengthy. Information briefs related to immigration cases took a median of 460 calendar days for an application filed in Canada, 620 days for those filed from the United States and 161 days for those filed abroad. Information briefs related to permanent resident applicants who are refugees in Canada had a median turnaround time of 442 days, and those for files subject to the Front-End Screening program had a turnaround time of 365 days. For inadmissibility briefs, SIRC noted similar median times.

¹⁶ This includes permanent residents from within and outside Canada (excluding the Refugee Determination Program), permanent residents from within the United States and applicants from overseas.

¹⁷ Individuals who arrive at the Canadian border or other ports of entry claiming refugee status.

¹⁸ Refugees, as defined by *IRPA*, who apply from within Canada for permanent resident status.

Table 6 provides a three-year highlight of the Service's median turnaround time in providing notices of assessment.

Table 6

Median turnaround time (in days) for notices of assessment

	2004–05	2005–06	2006–07
Citizenship	1	1	1
Immigration (Canada) ¹⁹	44	70	78
Immigration (USA) ²⁰	150	62	29
Overseas immigration	7	16	14
Refugee determination	56	96	98
Front-end screening	27	23	19

Other screening activities

In 2006–07, the Security Screening Branch vetted 114,500 visa applications of foreign nationals. The Branch also continued to provide screening for various site-access programs. For more information on this branch's security screening activities, refer to SIRC Review 2006–07 in this year's annual report.

New programs

The Security Screening Branch was involved in three new programs:

- **The Marine Facilities Restricted Area Access Control Program**—designed to provide security assessments to ensure security of Canada's ports;
- **The Trusted Traveller Program**—a pre-clearance program for travellers who travel frequently to the United States. This program is currently under development and there is no date set for its implementation; and
- **Passenger Protect**—the Branch worked with other government departments in the development of airline passenger screening programs, in particular the domestic “no fly” program, which became operational on June 18, 2007.

¹⁹ This includes certain classes of individuals who apply for permanent resident status within Canada.

²⁰ This includes persons who have been legally admitted to Canada for at least one year, and who may submit their application to Citizenship and Immigration offices in the United States.

INTELLIGENCE ASSESSMENTS BRANCH

The Intelligence Assessments Branch (formerly Research, Analysis and Production) consolidates the key analytical function of the Service and centralizes its main intelligence reporting mechanisms. It develops strategic and operational analyses of current threats and emerging issues, and produces Intelligence Briefs, Threat and Risk Assessments, Studies and Pathfinders.

This branch also has a role in the Terrorist Entity Listing process. Every two years, the Minister of Public Safety is obliged, under the *Criminal Code*, to review the Terrorist Entity Listing to determine whether there are reasonable grounds to add or remove entities from the list. The Minister bases this assessment on Security Intelligence Reports prepared by CSIS. In 2006–07, the Branch developed two such reports. The Minister's review of the listing was completed and approved by the Governor-in-Council on November 9, 2006.

HUMAN SOURCES AND OPERATIONS SUPPORT BRANCH

This branch provides a range of support and coordination services including risk management for operational activities across the Service. It is the policy centre in a number of areas including operational security, multilingual services and management of human sources. It also houses the Threat Management Centre, which provides 24/7 support to operational staff in headquarters, regional offices and foreign offices, and coordinates the Service's participation in major events such as the upcoming 2010 Winter Olympic Games in Vancouver.

SCIENTIFIC AND TECHNICAL SERVICES BRANCH

This branch develops and deploys technical tools and mechanisms to support the operations and investigations of CSIS's other branches.

INTEGRATED THREAT ASSESSMENT CENTRE

The Integrated Threat Assessment Centre (ITAC) produces assessments that warn the government about terrorist threats to Canada and to Canadian interests abroad. Once completed, ITAC's threat assessments are distributed to domestic and foreign partners. Additionally, ITAC acts as a distribution hub for threat assessments produced by counterparts in the United States, the United Kingdom, Australia and New Zealand.²¹

²¹ For more information about ITAC, refer to Section 1 of SIRC's 2005–06 Annual Report.

During the period under review, ITAC issued 83 threat assessments and redistributed 1,150 others produced by allied fusion centres. ITAC also began publishing *Media Watch* advisories at the beginning of the fiscal year, which are published each business day for distribution to clients. Further, ITAC provided 90 threat assessment briefings to its domestic clients. Presentations were provided to several government departments, including the Canada Revenue Agency and the Canada Border Services Agency. Also of note, ITAC produced one threat assessment at the request of the National Security Advisor.

In its previous annual report, SIRC observed that ITAC was not fully staffed but ITAC reported that as of March 31, 2007, the Centre was fully staffed.

2. Operations

Since the May 2006 realignment, each operational branch is responsible for investigating all threats emanating from within their respective geographic areas, with the exception of the International Terrorism Branch, which focuses exclusively on al Qaida and al Qaida-inspired groups regardless of geographic boundaries.

INTERNATIONAL TERRORISM BRANCH

This branch conducts investigations globally and within Canada, focusing on Islamist extremists engaged in a variety of terrorist-related activities which pose a direct threat to Canadians and Canadian interests. Notable among this branch's areas of interest is the radicalization of Islamists within Canada.

MIDDLE EAST AND AFRICA BRANCH

The Middle East and Africa Branch concentrates its investigative effort on threats that emanate from, or have as their major focus in, Middle East and African countries. This includes issues of terrorism, foreign-influenced activities, the proliferation of weapons of mass destruction and espionage.

ASIA, EUROPE AND AMERICAS BRANCH

This branch investigates threats emanating from its vast area of geographic responsibility, namely espionage, terrorism (including domestic extremism) transnational criminal activity and foreign-influenced activities.

INTERNATIONAL REGION

The International Region (formerly Foreign Liaison and Visits) manages the Service's liaison with foreign agencies and coordinates visits to CSIS Headquarters and CSIS regional offices by foreign representatives. It is also responsible for coordinating all Section 17(1) arrangements with foreign security intelligence or law enforcement agencies, as well as the operation of Foreign Officer posts abroad.

As part of CSIS's realignment, a new category of position, Foreign Officers (FO), was created. FO is the Service's generic term for any CSIS employee working at a post or mission abroad. FOs can include the formerly named Security Liaison Officers, the administrative assistants who support them, temporary duty officers who are working in a post, technical officers assigned to a post, and foreign secondment officers. FOs duties include:

- Management and collection of information on threats to the security of Canada;
- Management and collection of immigration security assessments;
- Liaison with foreign governments or institutions; and
- Collaborating and sharing information with staff at Canada's missions abroad.

The Service relies on these foreign posts to assist in liaising with foreign security and intelligence agencies, as well as to coordinate visits to CSIS Headquarters and regional offices by foreign representatives. SIRC's most recent examination of one of these foreign posts is summarized in SIRC Review 2006–01 in this year's annual report.

FEDERAL COURT WARRANTS AND WARRANT STATISTICS

Warrants are one of the most powerful and intrusive tools available to the Service. They provide CSIS with Federal Court authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telephone communications. For this reason, the use of warrants by CSIS is an important aspect of SIRC's reviews.

Each year, SIRC collects statistics on the Service's warrant applications and on warrants granted by the Federal Court under Sections 12 and 16 of the *CSIS*

Act. SIRC does not have the resources to examine all warrants granted to the Service. It does, however, look at a certain number of warrants as part of its annual review activity.

When SIRC examines a warrant, it looks into all aspects of the warrant process, starting with the development of the warrant application. SIRC verifies whether:

- the warrant application accurately reflected the information held by CSIS;
- CSIS's justification for requesting warrant powers was reasonable; and
- CSIS complied with the applicable legal and policy requirements in applying for warrant powers.

SIRC also looks at the actual warrant approved by the Federal Court and the Service's execution of warrant powers (i.e., how the warrant powers were used by CSIS).

Table 7
Warrant Statistics

	2004–05	2005–06	2006–07
New warrants	40	24	42
Replaced or renewed	207	203	134
Total	247	227	176*

* Included in this number were 25 urgent warrants.

In 2006–07, the Federal Court approved 42 new warrants—almost twice as many as the previous year. However, the Federal Court approved the renewal or replacement of only 134 warrants—a sharp drop from 203 reported in the previous year. Forty-two warrants were either terminated or expired without being renewed during the same period. No warrant applications were denied and all warrant powers requested by the Service were granted by the Federal Court.

In SIRC's 2005–06 annual report, SIRC reported on CSIS's review of the warrant process, which stemmed from a moratorium imposed by the Director after a warrant application was rejected by the Federal Court.²² During this moratorium—in effect from June 22, 2005 to June 28, 2006—there were 38 warrants approved on an exceptional basis by the Director and the Service's General Counsel. As a result of a year-long assessment of the warrant process, CSIS reported to SIRC that it is finalizing a streamlined approach to warrant review which is expected to be in effect by late 2007.

In preparing this report, SIRC asked the Service if the Federal Court had asked for any warrant applications to be modified before they were approved. Three instances were reported.

²² For more information on the moratorium, see "Federal Court Warrant and Warrant Statistics" in Section 2 of SIRC's 2005–06 Annual Report.

Section 3

About SIRC

About SIRC

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Gary Filmon, P.C., O.M., who was appointed on June 24, 2005. The other Members are the Honourable Raymond Speaker, P.C., O.C., the Honourable Baljit S. Chadha, P.C., the Honourable Roy Romanow, P.C., O.C., Q.C. and the Honourable Aldéa Landry, P.C., C.M., Q.C.

All Members of SIRC are Privy Councillors, who are appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties.

SIRC provides assurance to Parliament—and through it, to Canadians—that CSIS complies with legislation, policy and Ministerial Direction in the performance of its duties and functions. SIRC seeks to ensure that the Service does not undermine the fundamental rights and freedoms of Canadians. It is the only independent, external body with the legal mandate and expertise to review the activities of CSIS. Moreover, SIRC is a cornerstone of Canada's democratic tradition as it ensures the accountability of one of the government's most powerful organizations.

In addition to attending monthly committee meetings, members preside over complaints hearings, direct staff to undertake reviews, prepare complaint reports in consultation with staff, visit CSIS regional offices, appear before Parliament and exercise other duties associated with their responsibilities.

SIRC meetings and briefings 2006–07

April 5, 2006: The Chair spoke to the Associates of the I.H. Asper School of Business at the University of Manitoba in Winnipeg.

May 1, 2006: The Associate Executive Director and the Senior Counsel met with a delegation from the Czech Parliament.

May 12, 2006: The Chair and Executive Director delivered a presentation to Federal Court Judges regarding SIRC's warrant reviews.

June 8, 2006: The Associate Executive Director and Senior Researchers attended the third Review Agencies Forum hosted by the Inspector General of CSIS. In attendance were officials from the Commissioner of the Communications Security Establishment, the Inspector General of CSIS, and the Commission for Public Complaints Against the RCMP.

September 19, 2006: The Executive Director, the Associate Executive Director and the Senior Counsel met with Sir Peter Gibson, UK Intelligence Services Commissioner, his assistant David Massam and a representative from the UK High Commission.

September 22, 2006: The Chair spoke to the Global Business Forum in Banff, Alberta.

September 26, 2006: The Executive Director, the Associate Executive Director and the Senior Counsel met with a Norwegian Parliamentary Committee.

Continued on the next page

SIRC meetings and briefings 2006–07

(continued)

October 2–4, 2006: The Chair, one Committee Member and the Executive Director attended the International Intelligence Review Agencies Conference in Cape Town, South Africa. The Chair also participated in a panel discussion.

October 10, 2006: The Executive Director spoke at a Carleton University seminar on Intelligence, Statecraft and International Affairs.

October 26–28, 2006: The Executive Director and several staff attended the annual conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa.

November 1, 2006: The Chair, the Members of the Committee, the Executive Director, the Associate Executive Director and the Senior Counsel appeared before the Standing Committee on Public Safety and National Security of the House of Commons.

November 17, 2006: The Executive Director spoke at a Carleton University seminar entitled National Security and Intelligence in the Modern State.

December 10, 2006: The Chair appeared on CTV's *Question Period*.

January 31, 2007: The Associate Executive Director, Senior Counsel and Senior Researchers attended the fourth Review Agencies Forum, hosted by the Commission for Public Complaints Against the RCMP.

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 20, located in Ottawa. The staff comprises: an Associate Executive Director, Senior Counsel, a Senior Advisor, a Corporate Services Manager, Counsel, a Senior Paralegal (who also serves as Access to Information and Privacy Officer/Analyst), plus researchers and administrative staff.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

As part of their ongoing work, the Chair of SIRC, Committee Members and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of the security intelligence community. These exchanges are supplemented by discussions with academics, and other experts.

SIRC also visits CSIS regional offices on a rotating basis to examine the day-to-day work of investigators in the field. These trips give Committee Members an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. It is also an opportunity to communicate SIRC's focus and concerns.

During 2006–07, SIRC visited two regional offices.

BUDGET AND EXPENDITURES

SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee meetings, hearings, briefings and review activities represent SIRC's chief expenditures. Table 8 below presents a breakdown of actual and estimated expenditures.

Table 8
SIRC expenditures 2006–07

	2006–07 (Actual)	2006–07 (Estimates)
Personnel	\$1,817,160	\$1,777,000
Goods and Services	\$809,674	\$1,019,000
Total	\$2,626,834	\$2,796,000

INQUIRIES UNDER THE ACCESS TO INFORMATION AND PRIVACY ACTS

The public may make requests to SIRC under both the *Access to Information Act* and the *Privacy Act*. Table 9 outlines the number of requests SIRC has received under these Acts for the past three fiscal years.

Requests for SIRC's reviews represent the largest portion of these requests. SIRC waives the application fees for all such requests.

Table 9
Requests for release of information

	2004–05	2005–06	2006–07
<i>Access to Information Act</i>	21	17	12
<i>Privacy Act</i>	3	5	2

COMMUNICATIONS

Although SIRC's annual report is the main communications vehicle for informing Parliament and Canadians about its work, it has also implemented a modest communications program. SIRC has also undertaken some public opinion research, which shows that Canadians' awareness of review bodies remains very low, although perceptions of their independence and objectivity remain positive.

On occasion, the Committee is invited to attend and speak at conferences. In September 2006, the Chair delivered a speech to the Global Business Forum in Banff, Alberta, concerning “Global Threats to National Security.” In it, he examined the impact of the current threat environment on Canada’s economic security and well-being, described CSIS’s role in combating such threats and explained SIRC’s review functions.

In October 2006, the Chair delivered a speech on “Country Experiences: Oversight Mechanisms, Challenges and Opportunities” at the International Intelligence Review Agencies Conference, held in Cape Town, South Africa. This biannual conference brings together review agencies similar to SIRC to discuss issues of common concern. The Executive Director and another Member of the Committee were also in attendance.

SIRC’s website represents another important communications vehicle. It is continually updated with information relevant to the security and intelligence community. All of SIRC’s annual reports since its creation are available, plus copies of speeches, backgrounders and other publications, as well as information on the roles and responsibilities of SIRC.

As principal spokesperson, SIRC’s Chair has met with journalists to discuss SIRC’s work and appeared on CTV’s *Question Period*. He also wrote an op-ed piece, which was published in the *Calgary Herald*.

MANAGEMENT ACCOUNTABILITY

SIRC continues to make progress in this area, although as a very small federal agency without dedicated staff responsible for financial and human resource management, SIRC must increasingly rely on external contractors, diverting resources from its core functions.

In 2006–07, SIRC developed a financial management framework to improve the allocation and monitoring of expenditures. The latter aspect has been delayed, however, by technical problems related to software transition, preventing SIRC from realizing the full benefits of a modernized and automated monitoring of its expenditures.

In June 2006, SIRC received the results of an independent, external audit, which was a condition of receiving additional funding approved by Parliament in 2004. This audit found that “SIRC’s internal processes are reasonably well-controlled, thus enabling SIRC to properly manage the expenditure of public funds with prudence and probity.” Coincidentally, the Treasury Board Secretariat initiated

another audit of hospitality and travel expenses of small federal agencies and included SIRC in its ambit. The results of this second audit are expected to be published by the Treasury Board Secretariat in the coming year.

Following the successful development of a Management Action Plan and Risk Assessment in 2004–05, SIRC participated in an online reporting exercise under the government-wide Management Accountability Framework. The results of this exercise will be published by the Treasury Board Secretariat.

Also, SIRC completed a threat and risk assessment by an accredited security officer from the Privy Council Office to ensure compliance with the Management of Information Technology Security initiative. SIRC has also enhanced physical security by upgrading its alarm system and further shielding its hearing room.

Appendix A

SIRC reviews since 1984

SIRC reviews since 1984

This listing is also available on the SIRC website at www.sirc-csars.gc.ca.
Section 54 reports—flagged with an *—are special reports the Committee makes to the Minister of Public Safety.

1. *Eighteen Months After Separation: An Assessment of CSIS Approach to Staffing Training and Related Issues* (SECRET) (86/87-01) *
2. *Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service* (SECRET) (86/87-02) *
3. *The Security and Intelligence Network in the Government of Canada: A Description* (SECRET) (86/87-03) *
4. *Ottawa Airport Security Alert* (SECRET) (86/87-05) *
5. *Report to the Solicitor General of Canada Concerning CSIS Performance of its Functions* (SECRET) (87/88-01) *
6. *Closing the Gaps: Official Languages and Staff Relations in the CSIS* (UNCLASSIFIED) (86/87-04) *
7. *Counter-Subversion: SIRC Staff Report* (SECRET) (87/88-02)
8. *SIRC Report on Immigration Screening* (SECRET) (87/88-03) *
9. *Report to the Solicitor General of Canada on CSIS Use of Its Investigative Powers with Respect to the Labour Movement* (PUBLIC VERSION) (87/88-04) *
10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process* (SECRET) (88/89-01) *
11. *SIRC Review of the Counter-Terrorism Program in the CSIS* (TOP SECRET) (88/89-02) *
12. *Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS* (SECRET) (89/90-02) *

13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement* (SECRET) (89/90-03) *
14. *A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information* (SECRET) (89/90-04)
15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information* (SECRET) (89/90-05) *
16. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons* (UNCLASSIFIED) (89/90-06)
17. *SIRC Report on the Innu Interview and the Native Extremism Investigation* (SECRET) (89/90-07) *
18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988* (SECRET) (89/90-01) *
19. *A Review of the Counter-Intelligence Program in the CSIS* (TOP SECRET) (89/90-08) *
20. *Domestic Exchanges of Information* (SECRET) (90/91-03) *
21. *Section 2(d) Targets—A SIRC Study of the Counter-Subversion Branch Residue* (SECRET) (90/91-06)
22. *Regional Studies* (six studies relating to one region) (TOP SECRET) (90/91-04)
23. *Study of CSIS Policy Branch* (CONFIDENTIAL) (90/91-09)
24. *Investigations, Source Tasking and Information Reporting on 2(b) Targets* (TOP SECRET) (90/91-05)
25. *Release of Information to Foreign Agencies* (TOP SECRET) (90/91-02) *
26. *CSIS Activities Regarding Native Canadians—A SIRC Review* (SECRET) (90/91-07) *
27. *Security Investigations on University Campuses* (TOP SECRET) (90/91-01) *

28. *Report on Multiple Targeting* (SECRET) (90/91-08)
29. *Review of the Investigation of Bull, Space Research Corporation and Iraq* (SECRET) (91/92-01)
30. *Report on Al Mashat's Immigration to Canada* (SECRET) (91/92-02) *
31. *East Bloc Investigations* (TOP SECRET) (91/92-08)
32. *Review of CSIS Activities Regarding Sensitive Institutions* (TOP SECRET) (91/92-10)
33. *CSIS and the Association for New Canadians* (SECRET) (91/92-03)
34. *Exchange of Information and Intelligence between CSIS and CSE, Section 40* (TOP SECRET) (91/92-04) *
35. *Victor Ostrovsky* (TOP SECRET) (91/92-05)
36. *Report on Two Iraqis—Ministerial Certificate Case* (SECRET) (91/92-06)
37. *Threat Assessments, Section 40 Study* (SECRET) (91/92-07) *
38. *The Attack on the Iranian Embassy in Ottawa* (TOP SECRET) (92/93-01) *
39. "STUDYNT" *The Second CSIS Internal Security Case* (TOP SECRET) (91/92-15)
40. *Domestic Terrorism Targets—A SIRC Review* (TOP SECRET) (90/91-13) *
41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations* (TOP SECRET) (91/92-18)
43. *CSIS Activities during the Gulf War: Community Interviews* (SECRET) (90/91-12)
44. *Review of CSIS Investigation of a Latin American Illegal* (TOP SECRET) (90/91-10) *

45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985*—A SIRC Review (TOP SECRET) (91/92-14) *
46. *Prairie Region—Report on Targeting Authorizations* (Chapter 1) (TOP SECRET) (90/91-11) *
47. *The Assault on Dr. Hassan Al-Turabi* (SECRET) (92/93-07)
48. *Domestic Exchanges of Information* (A SIRC Review—1991/92) (SECRET) (91/92-16)
49. *Prairie Region Audit* (TOP SECRET) (90/91-11)
50. *Sheik Rahman's Alleged Visit to Ottawa* (SECRET) (CT 93-06)
51. *Regional Audit* (TOP SECRET) (September 1993)
52. *A SIRC Review of CSIS SLO Posts* (London & Paris) (SECRET) (91/92-11)
53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)
54. *Intelligence-Source Confidentiality* (TOP SECRET) (CI 93-03)
55. *Domestic Investigations* (1) (SECRET) (CT 93-02)
56. *Domestic Investigations* (2) (TOP SECRET) (CT 93-04)
57. *Middle East Movements* (SECRET) (CT 93-01)
58. *A Review of CSIS SLO Posts* (1992-93) (SECRET) (CT 93-05)
59. *Review of Traditional CI Threats* (TOP SECRET) (CI 93-01)
60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)
61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)
62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 93-11)

-
64. *Sources in Government* (TOP SECRET) (CI 93-09)
 65. *Regional Audit* (TOP SECRET) (CI 93-02)
 66. *The Proliferation Threat* (SECRET) (CT 93-07)
 67. *The Heritage Front Affair. Report to the Solicitor General of Canada* (SECRET) (CT 94-02) *
 68. *A Review of CSIS' SLO Posts* (1993-94) (SECRET) (CT 93-09)
 69. *Domestic Exchanges of Information* (A SIRC Review 1993-94) (SECRET) (CI 93-08)
 70. *The Proliferation Threat—Case Examination* (SECRET) (CT 94-04)
 71. *Community Interviews* (SECRET) (CT 93-11)
 72. *An Ongoing Counter-Intelligence Investigation* (TOP SECRET) (CI 93-07) *
 73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)
 74. *A SIRC Review of CSIS SLO Posts* (1994-95) (SECRET) (CT 95-01)
 75. *Regional Audit* (TOP SECRET) (CI 93-10)
 76. *Terrorism and a Foreign Government* (TOP SECRET) (CT 94-03)
 77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)
 78. *Review of Certain Foreign Intelligence Services* (TOP SECRET) (CI 94-02)
 79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 94-01)
 80. *Domestic Exchanges of Information* (A SIRC Review 1994-95) (SECRET) (CI 94-03)
 81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)
 82. *CSIS and a "Walk-In"* (TOP SECRET) (CI 95-04)
-

83. *A Review of a CSIS Investigation Relating to a Foreign State* (TOP SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 95-05)
85. *Regional Audit* (TOP SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats* (TOP SECRET) (CI 95-03)
87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)
88. *Homeland Conflict* (TOP SECRET) (CT 96-01)
89. *Regional Audit* (TOP SECRET) (CI 96-01)
90. *The Management of Human Sources* (TOP SECRET) (CI 96-03)
91. *Economic Espionage I* (SECRET) (CI 96-02)
92. *Economic Espionage II* (TOP SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996–97* (TOP SECRET) (CI 96-04)
94. *Urban Political Violence* (SECRET) (SIRC 1997-01)
95. *Domestic Exchanges of Information* (1996–97) (SECRET) (SIRC 1997-02)
96. *Foreign Conflict—Part I* (SECRET) (SIRC 1997-03)
97. *Regional Audit* (TOP SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1997-05)
99. *Spy Case* (TOP SECRET) (SIRC 1998-02)
100. *Domestic Investigations* (3) (TOP SECRET) (SIRC 1998-03)
101. *CSIS Cooperation with the RCMP—Part I* (SECRET) (SIRC 1998-04) *

102. *Source Review* (TOP SECRET) (SIRC 1998-05)
103. *Interagency Cooperation Case* (TOP SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest* (TOP SECRET) (SIRC 1998-08)
105. *CSIS Role in Immigration Security Screening* (SECRET) (CT 95-06)
106. *Foreign Conflict—Part II* (TOP SECRET) (SIRC 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)
108. *CSIS Cooperation with the RCMP—Part II* (SECRET) (SIRC 1998-04) *
109. *Audit of Section 16 Investigations and Foreign Intelligence 1997–98*
(TOP SECRET) (SIRC 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)
111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)
113. *Allegations by a Former CSIS Employee* (TOP SECRET) (SIRC 1998-12) *
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET)
(SIRC 1998-15)
116. *Files* (TOP SECRET) (SIRC 1998-16)
117. *Audit of Section 16 Investigations and Foreign Intelligence*
(TOP SECRET) (SIRC 1999-01)
118. *A Long-Running Counter Intelligence Investigation* (TOP SECRET)
(SIRC 1999-02)
119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)
120. *Proliferation* (TOP SECRET) (SIRC 1999-04)

121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—Bill C-31* (PROTECTED) (SIRC 1999-05) *
122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)
123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999-07)
124. *Regional Audit* (TOP SECRET) (SIRC 1999-08)
125. *Foreign State Activities* (TOP SECRET) (SIRC 1999-09)
126. *Project Sidewinder* (TOP SECRET) (SIRC 1999-10) *
127. *Security Breach* (TOP SECRET) (SIRC 1999-11)
128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET) (SIRC 2000-01)
129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999–2000* (TOP SECRET) (SIRC 2000-02)
130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000-03)
131. *Regional Audit* (TOP SECRET) (SIRC 2000-04)
132. *Warrant Review* (TOP SECRET) (SIRC 2000-05)
133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000* (TOP SECRET) (SIRC 2001-02)
134. *CSIS Investigation of Sunni Islamic Extremism* (TOP SECRET) (SIRC 2002-01)
135. *Source Recruitment* (TOP SECRET) (SIRC 2001-01)
136. *Collection of Foreign Intelligence* (TOP SECRET) (SIRC 2001-05)
137. *Domestic Extremism* (TOP SECRET) (SIRC 2001-03)
138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TOP SECRET) (SIRC 2001-04)

139. *Warrant Review* (TOP SECRET) (SIRC 2001-06)
140. *Special Report following allegations pertaining to an individual* (TOP SECRET) *
141. *Audit of Section 16 and Foreign Intelligence Reports* (TOP SECRET) (SIRC 2002-02)
142. *Review of the Ahmed Ressam Investigation* (TOP SECRET) (SIRC 2002-03)
143. *Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the Anti-Globalization Movement* (TOP SECRET) (SIRC 2002-04)
144. *Regional Audit* (TOP SECRET) (SIRC 2002-05)
145. *Special Report (2002-2003) following allegations pertaining to an individual* (TOP SECRET) *
146. *Front End Screening Program* (TOP SECRET) (SIRC 2003-01)
147. *CSIS Section 12 Operational Activity Outside Canada* (TOP SECRET) (SIRC 2003-02)
148. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2003-03)
149. *Review of a Counter-Proliferation Investigation* (TOP SECRET) (SIRC 2003-04)
150. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2003-05)
151. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2004-01)
152. *Review of CSIS's Investigation of Transnational Criminal Activity* (TOP SECRET) (SIRC 2004-02)
153. *Review of the Terrorist Entity Listing Process* (SECRET) (SIRC 2004-03)

154. *Review of Activities and Investigations in a CSIS Regional Office* (TOP SECRET) (SIRC 2004-04)
155. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2004-05)
156. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2004-06)
157. *Review of CSIS's Investigation of Threats against Canada's Critical Information Infrastructure* (TOP SECRET) (SIRC 2004-07)
158. *Review of CSIS's Exchanges of Information with Close Allies* (TOP SECRET) (SIRC 2004-08)
159. *Review of a Counter Proliferation Investigation* (TOP SECRET) (SIRC 2004-09)
160. *Terrorist Financing Activities in Canada* (TOP SECRET) (SIRC 2004-10)
161. *Section 54 Report to the Minister of Public Safety and Emergency Preparedness* (TOP SECRET) *
162. *Review of a Counter Terrorism Investigation* (TOP SECRET) (SIRC 2005-01)
163. *CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post* (TOP SECRET) (SIRC 2005-02)
164. *Review of the Integrated Threat Assessment Centre* (TOP SECRET) (SIRC 2005-03)
165. *Review of a Counter-Intelligence Investigation* (TOP SECRET) (SIRC 2005-04)
166. *Section 54 Report to the Minister of Public Safety: Review of the case of Mohammed Mansour Jabarah* (TOP SECRET) (SIRC 2005-05) *
167. *Review of Foreign Arrangements with Countries Suspected of Human Rights Violations* (TOP SECRET) (SIRC 2005-06)

168. *Review of CSIS's Electronic-Surveillance and Information-Gathering Techniques* (TOP SECRET) (SIRC 2005-07)
169. *Review of Activities and Investigations in a CSIS Region* (TOP SECRET) (SIRC 2005-08)
170. *Review of a Security Liaison Post* (TOP SECRET) (SIRC 2006-01)
171. *Review of Activities and Investigations in a CSIS Regional Office* (TOP SECRET) (SIRC 2006-02)
172. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2006-03)
173. *Review of a Section 16 activity* (TOP SECRET) (SIRC 2006-04)
174. *Review of a Counter-Terrorism Investigation* (TOP SECRET) (SIRC 2006-05)
175. *Review of CSIS's collaboration and exchanges of intelligence post-9/11* (TOP SECRET) (SIRC 2006-06)
176. *Review of Security Screening outside of the Federal Government* (TOP SECRET) (SIRC 2006-07)
177. Review 2006-08 had not been finalized at the time this annual report went to print. A summary of this review will appear in SIRC's 2007-08 annual report.
178. *Review of the CSIS Counter Espionage Investigations Desk* (TOP SECRET) (SIRC 2006-09)

Appendix B

Recommendations

Recommendations

During 2006–07, SIRC made 19 recommendations, 8 stemming from reviews it conducted and 11 from complaints investigations. These are summarized below.

	SIRC recommended that...
Review 2005-05	<ul style="list-style-type: none"> • The 1987 Memorandum of Understanding between CSIS and the Department of Foreign Affairs and International Trade be updated to designate Foreign Affairs as the lead agency in cases involving Canadian citizens detained abroad. • CSIS amend its policies so that emails are automatically retained unless there is a conscious decision to delete them. • CSIS clearly communicate to its employees what would constitute “recorded information,” as distinct from “transitory records,” and should therefore be filed and retained under applicable federal legislation. • Whenever possible, CSIS keep written records of its interdepartmental consultations, including but not limited to its formal and informal consultations with the Departments of Foreign Affairs and Justice. • CSIS ensure that the storage, retention and retrieval of all operational information under its control, including email messages, is in accordance with applicable federal legislation, including the <i>CSIS, Privacy, Access to Information and Library and Archives of Canada Acts</i>. • CSIS request and obtain written advice from the Department of Justice in operations where an individual is questioned in circumstances which may give rise to a detention, in order to ensure that the individual's <i>Charter</i> rights are respected, and in all occasions when it is unclear whether the Service's activity falls within its statutory mandate under Section 12 of the <i>CSIS Act</i>.
Review 2006-07	<ul style="list-style-type: none"> • CSIS create policy to address the varying degrees of risk of screening applicants, and to ensure that these briefs are uniform and consistent. • CSIS obtain written consent forms for security assessments in cases where the Service cannot access them after the fact (i.e. foreign agencies).

	SIRC recommended that...
Report 2006-01	<ul style="list-style-type: none"> • The Canadian Human Rights Commission not investigate this complaint.
Report 2006-02	<ul style="list-style-type: none"> • CSIS implement a procedure to verify that individuals about to be interviewed by CSIS for citizenship or immigration interviews be given adequate written notice by Citizenship and Immigration Canada that CSIS intends to interview them.
Report 2006-03	<ul style="list-style-type: none"> • CSIS create and implement a policy requiring that its employees be informed of their right to legal representation and be given an opportunity to consult with a legal representative before and while an interview is conducted for the purposes of either a breach of security or a breach of conduct investigation. • CSIS create a roster of lawyers from the private sector who have a Top Secret clearance whom CSIS employees may retain. • CSIS create and implement a policy by which its investigators must declare a conflict of interest when an individual seeks their opinion about the retention of legal counsel. • CSIS create and implement a policy requiring that its employees input relevant information in a timely manner. • CSIS amend its policy dealing with the destruction of investigative materials—including audio-cassettes and notes—concerning a breach of security investigation or a disciplinary investigation. • CSIS remind its employees that SIRC has the statutory right to access all information under the control of CSIS—except for matters of Cabinet confidence—including audio cassettes, handwritten notes and email messages, and that care should be taken to not destroy information that could have an impact on SIRC's ability to exercise its right to access such information. • CSIS place greater emphasis on employees' obligations with respect to the protection of classified information in its orientation course and other security briefings.
Report 2006-04	<ul style="list-style-type: none"> • CSIS formally retract a statement and that it do so by informing the Minister of Citizenship and Immigration, the Minister of Public Safety, the Federal Court of Canada and the publishers of two newspapers. • CSIS apologize to Human Concern International for having made an unsubstantiated statement.

Le CSARS a recommandé que...	
<ul style="list-style-type: none"> • La Commission canadienne des droits de la personne ne fasse pas enquête sur cette plainte. 	Rapport n° 2006-01
<ul style="list-style-type: none"> • Le SCRS instaure une procédure pour vérifier si les personnes à qui il est sur le point de faire subir une entrevue de citoyenneté ou d'immigration ont eu un préavis écrit suffisant de citoyenneté et Immigration Canada, les informant que le SCRS compte les interviewer. 	Rapport n° 2006-02
<ul style="list-style-type: none"> • Le SCRS élabore et met en œuvre une politique prescrivant que ses employés soient informés de leur droit à être représentés par un avocat et qu'ils aient la possibilité d'en consulter un avant et pendant une entrevue menée dans le cadre d'une enquête sur une infraction à la sécurité ou sur un écart de conduite. • Le SCRS dresse un répertoire des avocats du secteur privé qui sont titulaires d'une cote de sécurité « Très secret » et dont les services pourraient être retenus par les employés du SCRS. • Le SCRS élabore et met en œuvre une politique prescrivant à ses enquêteurs de faire état de tout conflit d'intérêts si quelqu'un leur demande leur opinion concernant les services d'un avocat à qui recourir. • Le SCRS élabore et met en œuvre une politique prescrivant à ses employés de fournir les renseignements pertinents en temps utile. • Le SCRS modifie sa politique relative à la destruction des documents d'enquête sur une infraction à la sécurité ou d'enquête disciplinaire, dont les audiocassettes et les notes. • Le SCRS rappelle à ses employés que la loi confère au CSARS le droit d'accès à toute information qui relève du SCRS – sauf les documents confidentiels du Cabinet – dont les audiocassettes, les notes manuscrites et les messages électroniques, et qu'il faut veiller à ne pas détruire des informations qui pourraient affecter la capacité du CSARS à exercer son droit d'accès à ces informations. • Le SCRS met davantage l'accent sur les obligations des employés relatives à la protection des renseignements classifiés, dans son cours d'orientation et dans les autres exposés sur la sécurité. 	Rapport n° 2006-03
<ul style="list-style-type: none"> • Le SCRS rétracte officiellement une déclaration, et ce, en informant le ministre de la Citoyenneté et de l'Immigration, le ministre de la Sécurité publique, la Cour fédérale du Canada et les éditeurs des deux journaux. • Le SCRS s'excuse auprès de Human Concern International d'avoir fait une déclaration non corroborée. 	Rapport n° 2006-04

Recommandations

Au cours de 2006-2007, le CSARS a formulé 19 recommandations, 8 découlant de ses études et 11, des enquêtes menées sur des plaintes. Voici le résumé de ces recommandations.

Le CSARS a recommandé que...	
Etude n° 2005-05	<ul style="list-style-type: none">• Le protocole d'entente conclu en 1987 entre le SCRS et le ministère des Affaires étrangères et du Commerce international soit mis à jour et désigne ce ministère à titre d'organisme principal dans les affaires de citoyens canadiens détenus à l'étranger.• Le SCRS modifie ses politiques de façon que les courriels soient conservés d'office, à moins d'une décision délibérée de les supprimer.• Le SCRS informe clairement ses employés de ce qu'est un « renseignement conigné », par opposition à « document éphémère », et du fait qu'il doit donc être classé et conservé selon les lois fédérales applicables.• Le SCRS conserve des documents de ses consultations interministérielles, dans la mesure du possible, y compris mais non de façon limitative de ses consultations officielles et non officielles auprès des ministères des Affaires étrangères et de la Justice.• Le SCRS veille à ce que le stockage, la conservation et la recherche de toutes les informations opérationnelles qui relèvent de lui, dont les courriels, soient conformes aux lois fédérales applicables, y compris les Lois sur le SCRS, sur la protection des renseignements personnels, sur l'accès à l'information et sur la Bibliothèque et les Archives du Canada.• Le SCRS demande et obtienne du ministère de la Justice un avis écrit pour toute opération amenant à interroger un individu dans des circonstances qui peuvent entraîner sa détention, afin d'assurer le respect des droits de l'intéressé en vertu de la Charte, et en toute occasion où il n'est pas clair que l'activité du Service entre dans son mandat selon l'article 12 de la Loi sur le SCRS.
Etude n° 2006-07	<ul style="list-style-type: none">• Le SCRS élabore une politique pour régler la question de la gradation correspondant aux divers degrés de risque posé par les postulants au filtrage et assurer que ces notes d'information soient uniformes et cohérentes.• Le SCRS obtienne des formulaires de consentement écrit aux évaluations de sécurité dans les cas où il ne peut y avoir accès après le fait (soit dans le cas des organismes étrangers).

Annexe B

Recommendations

173. *Review of a Section 16 activity* (TRÈS SECRET) (SIRC 2006-04)
174. *Étude d'une enquête antiterroriste* (TRÈS SECRET) (SIRC 2006-05)
175. *Review of CSIS's collaboration and exchanges of intelligence post 9/11* (TRÈS SECRET) (SIRC 2006-06)
176. *Review of Security Screening outside of the Federal Government* (TRÈS SECRET) (SIRC 2006-07)
177. L'étude n° 2006-08 n'était pas terminée au moment de mettre sous presse. Un résumé en sera présenté dans le Rapport annuel du CSARS 2007-2008.
178. *Review of the CSIS Counter Espionage Investigations Desk* (TRÈS SECRET) (SIRC 2006-09)

172. *Review of a Counter-Terrorism Investigation* (TRÈS SECRET) (SIRC 2006-03)
171. *Review of Activities and Investigations in a CSIS Regional Office* (TRÈS SECRET) (SIRC 2006-02)
170. *Review of a Security Liaison Post* (TRÈS SECRET) (SIRC 2006-01)
169. *Review of activities and investigations in a CSIS region* (TRÈS SECRET) (SIRC 2005-08)
168. *Review of CSIS's electronic-surveillance and information-gathering techniques* (TRÈS SECRET) (SIRC 2005-07)
167. *Review of foreign arrangements with countries suspected of human rights violence* (TRÈS SECRET) (SIRC 2005-06)
166. *Rapport en vertu de l'article 54 : Étude de l'affaire Mohammed Mansour Jabarah* (TRÈS SECRET) (SIRC 2005-05)
165. *Review of a counter-intelligence investigation* (TRÈS SECRET) (SIRC 2005-04)
164. *Review of the Integrated Threat Assessment Centre* (TRÈS SECRET) (SIRC 2005-03)
163. *CSIS liaison with foreign agencies: review of a security liaison post* (TRÈS SECRET) (SIRC 2005-02)
162. *Review of a counter-terrorism investigation* (TRÈS SECRET) (SIRC 2005-01)
161. *Section 54 Report to the Minister of Public Safety and Emergency Preparedness* (TRÈS SECRET)*
160. *Terrorist Financing Activities in Canada* (TRÈS SECRET) (SIRC 2004-10)
159. *Review of a Counter-Proliferation Investigation* (TRÈS SECRET) (SIRC 2004-09)
158. *Review of CSIS's Exchanges of Information with Close Allies* (TRÈS SECRET) (SIRC 2004-08)
157. *Review of CSIS's Investigation of Threats against Canada's Critical Information Infrastructure* (TRÈS SECRET) (SIRC 2004-07)

140. Rapport spécial sur des allégations concernant une personne (TRÈS SECRET)*
141. Audit of Section I6 and Foreign Intelligence Reports (TRÈS SECRET)
(SIRC 2002-02)
142. Review of the Ahmed Ressaam Investigation (TRÈS SECRET) (SIRC 2002-03)
143. Lawful Advocacy, Protest and Dissent Versus Serious Violence Associated with the
Anti-Globalization Movement (TRÈS SECRET) (SIRC 2002-04)
144. Regional Audit (TRÈS SECRET) (SIRC 2002-05)
145. Rapport spécial (2002-2003) sur des allégations concernant une personne
(TRÈS SECRET)*
146. Front End Screening Program (TRÈS SECRET) (SIRC 2003-01)
147. CSIS Section 12 Operational Activity Outside Canada (TRÈS SECRET)
(SIRC 2003-02)
148. Review of a Counter Intelligence Investigation (TRÈS SECRET) (SIRC 2003-03)
149. Review of a Counter Proliferation Investigation (TRÈS SECRET) (SIRC 2003-04)
150. CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post
(TRÈS SECRET) (SIRC 2003-05)
151. CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post
(TRÈS SECRET) (SIRC 2004-01)
152. Review of CSIS's Investigation of Transnational Criminal Activity
(TRÈS SECRET) (SIRC 2004-02)
153. Review of the Terrorist Entity Listing Process (SECRET) (SIRC 2004-03)
154. Review of Activities and Investigations in a CSIS Regional Office (TRÈS SECRET)
(SIRC 2004-04)
155. Review of a Counter Terrorism Investigation (TRÈS SECRET) (SIRC 2004-05)
156. Review of a Counter Intelligence Investigation (TRÈS SECRET) (SIRC 2004-06)

122. *Domestic Targets* (TRÈS SECRET) (SIRC 1999-06)
123. *Terrorist Fundraising* (TRÈS SECRET) (SIRC 1999-07)
124. *Regional Audit* (TRÈS SECRET) (SIRC 1999-08)
125. *Foreign State Activities* (TRÈS SECRET) (SIRC 1999-09)
126. *Le Projet Sidewinder* (TRÈS SECRET) (SIRC 1999-10)*
127. *Security Breach* (TRÈS SECRET) (SIRC 1999-11)
128. *Domestic Exchanges of Information 1999-2000* (TRÈS SECRET) (SIRC 2000-01)
129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999-2000* (TRÈS SECRET) (SIRC 2000-02)
130. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 2000-03)
131. *Regional Audit* (TRÈS SECRET) (SIRC 2000-04)
132. *Warrant Review* (TRÈS SECRET) (SIRC 2000-05)
133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999 2000* (TRÈS SECRET) (SIRC 2001-02)
134. *CSIS Investigation of Sunni Islamic Extremism* (TRÈS SECRET) (SIRC 2002-01)
135. *Source Recruitment* (TRÈS SECRET) (SIRC 2001-01)
136. *Collection of Foreign Intelligence* (TRÈS SECRET) (SIRC 2001-05)
137. *Domestic Extremism* (TRÈS SECRET) (SIRC 2001-03)
138. *CSIS Liaison with Foreign Agencies: Audit of an SLO Post* (TRÈS SECRET) (SIRC 2001-04)
139. *Warrant Review* (TRÈS SECRET) (SIRC 2001-06)

103. *Interagency Cooperation Case* (TRÈS SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest* (TRÈS SECRET) (SIRC 1998-08)
105. *Le rôle du SCRS dans le filtrage de sécurité des demandes d'immigration* (SECRET) (CT 95-06)
106. *Un conflit étranger, partie II* (TRÈS SECRET) (SIRC 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)
108. *Coopération du SCRS avec la GRC - partie II* (SECRET) (SIRC 1998-04)*
109. *Audit of Section 16 Investigations and Foreign Intelligence 1997-98* (TRÈS SECRET) (SIRC 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)
111. *Regional Audit* (TRÈS SECRET) (SIRC 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 1998-11)
113. *Allegations d'un ancien employé du SCRS* (TRÈS SECRET) (CSARS 1998-12)*
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TRÈS SECRET) (SIRC 1998-15)
116. *Files* (TRÈS SECRET) (SIRC 1998-16)
117. *Audit of Section 16 Investigations and Foreign Intelligence* (TRÈS SECRET) (SIRC 1999-01)
118. *A Long-Running Counter Intelligence Investigation* (TRÈS SECRET) (SIRC 1999-02)
119. *Domestic Exchanges of Information* (TRÈS SECRET) (SIRC 1999-03)
120. *Proliferation* (TRÈS SECRET) (SIRC 1999-04)
121. *Observations du CSARS sur le projet de loi C 31 dont est actuellement saisi le Parlement* (PROTÉGÉ) (SIRC 1999-05)*

84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 95-05)
85. *Vérification régionale* (TRÈS SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats* (TRÈS SECRET) (CI 95-03)
87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)
88. *Homeland Conflict* (TRÈS SECRET) (CT 96-01)
89. *Vérification régionale* (TRÈS SECRET) (CI 96-01)
90. *La gestion des sources humaines* (TRÈS SECRET) (CE 96-03)
91. *Economic Espionage I* (SECRET) (CI 96-02)
92. *Economic Espionage II* (TRÈS SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996-1997* (TRÈS SECRET) (CI 96-04)
94. *Urban Political Violence* (SECRET) (SIRC 1997-01)
95. *Domestic Exchanges of Information* (1996-97) (SECRET) (SIRC 1997-02)
96. *Conflit étrangers, partie I* (SECRET) (SIRC 1997-03)
97. *Regional Audit* (TRÈS SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 1997-05)
99. *Spy Case* (TRÈS SECRET) (SIRC 1998-02)
100. *Enquêtes menées au Canada* (3) (TRÈS SECRET) (CSARS 1998-03)
101. *Coopération du SCRS avec la Gendarmerie royale du Canada - partie I* (SECRET) (CSARS 1998-04)*
102. *Source Review* (TRÈS SECRET) (SIRC 1998-05)

83. *A Review of a CSIS Investigation relating to a Foreign State* (TRÈS SECRET) (CI 95-02)
82. *CSIS and a "Walk-In"* (TRÈS SECRET) (CI 95-04)
81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)
80. *Échanges d'information avec des organismes canadiens (enquête du CSARS 1994-1995)* (SECRET) (CI 94-03)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 94-01)
78. *Review of Certain Foreign Intelligence Services* (TRÈS SECRET) (CI 94-02)
77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)
76. *Terrorism and a Foreign Government* (TRÈS SECRET) (CT 94-03)
75. *Regional Audit* (TRÈS SECRET) (CI 93-10)
74. *A SIRC Review of CSIS' SLO Posts (1994-95)* (SECRET) (CT 95-01)
73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)
72. *Une enquête suivie en matière de contre-espionnage* (TRÈS SECRET) (CE 93-07)*
71. *Community Interviews* (SECRET) (CT 93-11)
70. *The Proliferation Threat – Case Examination* (SECRET) (CT 94-04)
69. *Échanges d'information avec des organismes canadiens (enquête du CSARS 1993-1994)* (SECRET) (CI 93 08)
68. *A Review of CSIS' SLO Posts (1993-94)* (SECRET) (CT 93-09)
67. *L'affaire du Héritage Front, rapport présenté au Solliciteur général du Canada* (SECRET) (AT 94-02)*
66. *The Proliferation Threat* (SECRET) (CT 93-07)
65. *Regional Audit* (TRÈS SECRET) (CI 93-02)

64. *Sources in Government* (TRÈS SECRET) (CI 93-09)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TRÈS SECRET) (CI 93-11)
62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)
61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)
60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)
59. *Review of Traditional CI Threats* (TRÈS SECRET) (CI 93-01)
58. *A Review of CSIS' SLO Posts (1992-93)* (SECRET) (CT 93-05)
57. *Middle East Movements* (SECRET) (CT 93-01)
56. *Enquêtes menées au Canada (2)* (TRÈS SECRET) (CT 93-04)
55. *Domestic Investigations (1)* (SECRET) (CT 93-02)
54. *Intelligence-Source Confidentiality* (TRÈS SECRET) (CI 93-03)
53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)
52. *Examen par le CSARS des bureaux des ALS du Service (Londres et Paris)* (SECRET) (91/92-11)
51. *Regional Audit* (TRÈS SECRET)
50. *La présunte venue du sheikh Rahman à Ottawa* (SECRET) (CT 93-06)
49. *Vérification de la région des Prairies* (TRÈS SECRET) (90/91-11)
48. *Domestic Exchanges of Information (A SIRCI Review – 1991/92)* (SECRET) (91/92-16)
47. *L'attentat contre Hassan El-Tounabi* (SECRET) (92/93-07)
46. *Région des Prairies – rapport sur les autorisations d'enquête (chapitre 1)* (TRÈS SECRET) (90/91-11) *

29. *Revue de l'enquête sur Bull, la Corporation de recherche spatiale et l'Iraq* (SECRET) (91/92-01)
30. *Rapport sur l'immigration d'Al Mashat au Canada* (SECRET) (91/92-02)*
31. *East Bloc Investigations* (TRÈS SECRET) (91/92-08)
32. *Review of CSIS Activities Regarding Sensitive Institutions* (TRÈS SECRET) (91/92-10)
33. *CSIS and the Association for New Canadians* (SECRET) (91/92-03)
34. *Echange d'informations et de renseignements entre le Service canadien du renseignement de sécurité et le Centre de la sécurité des télécommunications* (TRÈS SECRET) (91/92-04)*
35. *Victor Ostrovsky* (TRÈS SECRET) (91/92-05)
36. *Report on Iwo Iraqis – Ministerial Certificate Case* (SECRET) (91/92-06)
37. *Evaluations de la menace, étude en vertu de l'article 40* (SECRET) (91/92-07)*
38. *L'attaque contre l'ambassade de l'Iran à Ottawa* (TRÈS SECRET) (92/93-01)*
39. *"STUDYNT" The Second CSIS Internal Security Case* (TRÈS SECRET) (91/92-15)
40. *Les cibles du terrorisme national – un examen du CSARS* (TRÈS SECRET) (90/91-13)*
41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations* (TRÈS SECRET) (91/92-18)
43. *Activités du SCRS pendant la Guerre du Golfe : entrevues dans la communauté* (SECRET) (90/91-12)
44. *Examen de l'enquête menée par le SCRS sur un agent clandestin latino-américain – un examen du CSARS* (TRÈS SECRET) (90/91-10)*
45. *Les activités du SCRS relativement à la destruction de l'avion affecté au vol 182 d'Air India le 23 juin 1985 – un examen du CSARS* (TRÈS SECRET) (91/92-14)*

14. L'examen de la politique et des pratiques du SCRS concernant les divulgations non autorisées d'informations classifiées (SECRET) (89/90-04)
15. Report to the Solicitor General of Canada on Citizenship/Third Party Information (SECRET) (89/90-05)*
16. Modifications à la Loi sur le SCRS : propositions au Comité spécial de la Chambre des communes (NON CLASSIFIÉ) (89/90-06)
17. Rapport sur l'entrevue concernant les Innus et l'enquête sur l'extrémisme autochtone (SECRET) (89/90-07)*
18. Supplement to the Committee's Report on Immigration Screening of January 18, 1988 (SECRET) (89/90-01)*
19. A Review of the Counter-Intelligence Program in the CSIS (TRÈS SECRET) (89/90-08)*
20. Échanges de renseignements avec des organismes canadiens (SECRET) (90/91-03)*
21. Cibles établies en vertu de l'alinéa 2d) – une étude du CSARS sur les opérations restantes de la Direction de l'antisubversion (SECRET) (90/91-06)
22. Études régionales (six études sur une région) (TRÈS SECRET) (90/91-04)
23. Study of CSIS' Policy Branch (CONFIDENTIEL) (90/91-09)
24. Enquêtes, affectation de sources et rapport sur les cibles en vertu de l'alinéa 2b) (TRÈS SECRET) (90/91-05)
25. Communication de renseignements aux services étrangers (TRÈS SECRET) (90/91-02)*
26. Examen par le CSARS des activités du SCRS touchant les Canadiens autochtones (SECRET) (90/91-07)*
27. Enquêtes de sécurité sur les campus universitaires (TRÈS SECRET) (90/91-01)*
28. Report on Multiple Targeting (SECRET) (90/91-08)

Rapports et études du CSARS depuis 1984

Cette liste figure aussi sur le site Web du CSARS à www.sirc-csars.gc.ca. Les rapports marqués d'un astérisque (*) sont des documents spéciaux que le CSARS prépare à l'intention du ministre de la Sécurité publique en vertu de l'article 54.

1. Dix-huit mois après la séparation : une appréciation de la conception du SCRS sur le recrutement, le perfectionnement et les questions connexes (SECRET) (86/87-01)*
2. Rapport d'une étude portant sur le filtrage de sécurité des fonctionnaires et des personnes postulant un emploi dans la fonction publique fédérale (SECRET) (86/87-02)*
3. Le réseau du renseignement et de sécurité au sein de l'administration gouvernementale du Canada : une description (SECRET) (86/87-03)*
4. Alerte de sécurité à l'aéroport d'Ottawa (SECRET) (86/87-05)*
5. Report to the Solicitor General of Canada Concerning CSIS Performance of its Functions (SECRET) (87/88-01)*
6. Pour corriger une situation : langues officielles et relations de travail au sein du SCRS (NON CLASSIFIÉ) (86/87-04)*
7. Counter-Subversion: SIRC Staff Report (SECRET) (87/88-02)
8. Rapport du CSARS – Sélection des immigrants (SECRET) (87/88-03)*
9. L'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrir (VERSION PUBLIQUE) (87/88-04)*
10. La Direction de l'évaluation du renseignement : une revue par le CSARS du processus de production (SECRET) (88/89-01)*
11. CSARS – Examen du programme de l'antiterrorisme du SCRS (TRÈS SECRET) (88/89-02)*
12. Rapport présenté au Solliciteur général du Canada sur la protection des biens scientifiques et techniques au Canada : le rôle du SCRS (SECRET) (89/90-02)*
13. SIRC Report on CSIS Activities Regarding the Canadian Peace Movement (SECRET) (89/90-03)*

Annexe A

Rapports et études du CSARS depuis 1984

RESPONSABILISATION DE GESTION

Le Comité continue de faire des progrès sur ce plan, quoiqu'il doive de plus en plus faire appel à des entrepreneurs de l'extérieur, étant un organisme fédéral de très petite taille qui ne peut se payer le luxe d'avoir des employés chargés de gérer les ressources financières et humaines, ce qui accapare certaines ressources destinées à ses fonctions principales.

En 2006-2007, le CSARS a élaboré un cadre de gestion financière visant à améliorer l'affectation et le contrôle des dépenses. Des problèmes techniques liés à la transition au logiciel ont toutefois retardé ce dernier volet, empêchant le CSARS de profiter pleinement de tous les avantages d'un contrôle moderne et automatisé de ses dépenses.

En juin 2006, le CSARS a reçu les résultats d'une vérification indépendante de l'extérieur, qui était une condition de l'obtention des fonds supplémentaires approuvés par le Parlement en 2004. Selon ces résultats, « les processus internes du CSARS sont assez bien contrôlés, ce qui lui permet de gérer les dépenses de fonds publics comme il se doit, avec prudence et probité ». Parallèlement, le Secrétaire du Conseil du Trésor a en outre amorcé la vérification des frais de voyage et d'accueil des petits organismes fédéraux, dont le CSARS. Il devrait publier les résultats de cette deuxième vérification au cours de la prochaine année.

À la suite de l'élaboration fructueuse d'un plan d'action de la gestion et d'une évaluation des risques en 2004-2005, le CSARS a pris part à une reddition de comptes en ligne en vertu du Cadre de responsabilisation de gestion pangouvernemental. Le Secrétaire du Conseil du Trésor publiera les résultats de ces travaux.

Le CSARS a aussi fait réaliser une évaluation des menaces et des risques par un agent de sécurité accrédité du Bureau du Conseil privé pour s'assurer de sa conformité à l'initiative de Gestion de la sécurité des technologies de l'information. Il a aussi relevé la sécurité matérielle de ses locaux en améliorant son système d'alarme et en renforçant le blindage de sa salle d'audience.

COMMUNICATIONS

Même si son rapport annuel est le principal moyen d'informer le Parlement et les Canadiens au sujet de ses travaux, le Comité n'en a pas moins instauré un mode de programme de communication. En matière d'opinion publique, il a en outre mené des recherches dont les résultats montrent que les Canadiens sont encore très peu sensibilisés à la question des organismes de surveillance, quoique les perceptions quant à l'indépendance et à l'objectivité de ceux-ci demeurent positives.

À l'occasion, le Comité est invité à déléguer des représentants à des conférences pour y prendre la parole. En septembre 2006, le président a prononcé une allocution sur les menaces mondiales à la sécurité nationale devant le Global Business Forum, à Banff (Alberta). Il y a parlé de l'impact du contexte des menaces actuelles sur la sécurité économique et le bien-être du Canada, explorant le rôle du SCRS dans la lutte à ces menaces et expliquant les fonctions de surveillance du CSARS.

En octobre 2006, le président a prononcé une allocution sur les expériences de divers pays à l'égard des mécanismes de contrôle et des défis et possibilités en cette matière, à la conférence internationale des organismes de surveillance du renseignement tenue à Cape Town, en Afrique du Sud. Tous les deux ans, cette conférence réunit des organismes semblables au CSARS pour discuter de dossiers d'intérêt commun. Le directeur exécutif et un autre membre du Comité y ont aussi pris part.

Le site Web du CSARS constitue un autre moyen de communication important. Il est sans cesse mis à jour par une information pertinente à la collectivité de la sécurité et du renseignement. On y trouve tous les rapports annuels du CSARS depuis sa création, de même que le texte de discours, de documents d'information et d'autres publications, ainsi que la description des rôles et responsabilités du CSARS.

En qualité de porte-parole principal, le président a rencontré quelques journalistes pour discuter des travaux du CSARS et il a été reçu à l'émission « Question Period » du Réseau CTV. Il a aussi signé un article dans la section opinion de la page éditoriale du *Calgary Herald*.

BUDGET ET DÉPENSES

Le CSARS continue de gérer ses activités dans les limites des ressources qui lui sont octroyées. Ses principales dépenses ont trait au traitement et aux déplacements de son personnel au Canada pour prendre part aux réunions, audiences, exposés et activités d'examen du Comité. Le tableau 8 présente une ventilation des dépenses réelles et des prévisions à ce chapitre.

Tableau 8			
Dépenses du CSARS 2006-2007			
	2006-2007 (dépenses réelles)	2006-2007 (prévisions)	
Personnel	1 817 160 \$	1 777 000 \$	
Biens et services	809 674 \$	1 019 000 \$	
Total	2 626 834 \$	2 796 000 \$	

DEMANDES EN VERTU DES LOIS SUR L'ACCÈS À L'INFORMATION ET
SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le public peut présenter au CSARS des demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. Le tableau 9 fait état du nombre de demandes que ces lois ont values au Comité au cours des trois derniers exercices financiers.

Le gros de ces demandes concerne des études du Comité, qui ne perçoit de droits pour aucune d'elles.

Tableau 9			
Demandes de communication de renseignements			
	2004-2005	2005-2006	2006-2007
Loi sur l'accès à l'information	21	17	12
Loi sur la protection des renseignements personnels	3	5	2

PERSONNEL ET ORGANISATION

Le Comité jouit du soutien de son directeur exécutif, Susan Pollak, et d'un effectif autorisé de 20 employés, en poste à Ottawa. Son personnel est ainsi composé : un directeur exécutif associé, un avocat principal, un conseiller principal, un directeur des services généraux, un avocat, un parajuriste principal (qui est aussi agent/analyste à l'accès à l'information et à la protection des renseignements personnels), plus des chercheurs et des employés de soutien administratif.

Les membres du Comité dicent au personnel l'orientation à donner aux travaux de recherche et autres activités qui sont désignées prioritaires pour l'année. La marche des affaires courantes est confiée au directeur exécutif qui s'enquiert au besoin de la ligne de conduite à tenir auprès du président, premier dirigeant du CSARS.

Dans le cadre de leur travail courant, le président et les membres du Comité ainsi que les cadres supérieurs prennent part régulièrement à des discussions avec la direction et le personnel du SCRS et avec d'autres membres de haut rang de la collectivité du renseignement de sécurité. À ces échanges se greffent des discussions avec des universitaires et d'autres experts.

Les membres du Comité visitent aussi les bureaux régionaux du Service à tour de rôle pour examiner le travail courant des enquêteurs locaux. Ces visites leur fournissent l'occasion de se faire exposer les problèmes, difficultés et priorités propres à ces bureaux par le personnel sur place. Elles leur permettent aussi de faire valoir ce qui polarise les efforts et les préoccupations du CSARS.

Au cours de 2006-2007, les membres du CSARS se sont rendus dans deux bureaux régionaux.

Réunions et exposés du CSARS, 2006-2007 (suite)

2-4 octobre 2006 : Le président, un membre du Comité et le directeur exécutif assistent à la conférence internationale des organismes du renseignement à Cape Town, en Afrique du Sud. Le président participe aussi à un débat d'experts.

10 octobre 2006 : Le directeur exécutif prononce une allocution à un colloque tenu à l'Université Carleton sur le renseignement, l'habileté politique et les affaires internationales.

26-28 octobre 2006 : Le directeur exécutif et plusieurs membres du personnel assistent à la conférence annuelle de l'Association canadienne pour l'étude de la sécurité et du renseignement, tenue à Ottawa.

1^{er} novembre 2006 : Le président, les membres du Comité, le directeur exécutif, le directeur exécutif associé et l'avocat principal comparaissent devant le Comité permanent de la Chambre des communes sur la sécurité publique et nationale.

17 novembre 2006 : Le directeur exécutif prononce une allocution à un colloque de l'Université Carleton sur la sécurité nationale et le renseignement dans l'État moderne.

10 décembre 2006 : Le président est reçu à l'émission « Question Period » du Réseau CTV.

31 janvier 2007 : Le directeur exécutif associé, l'avocat principal et des chercheurs supérieurs assistent au quatrième Forum des organismes de surveillance, tenu par la Commission des plaintes du public contre la GRC.

COMPOSITION DU COMITÉ

La présidence du Comité est occupée par l'honorable Gary Filmon, C.R., O.M., nommé à cette charge le 24 juin 2005. Les autres membres sont l'honorable Raymond Speaker, C.R., O.C., l'honorable Baljit S. Chadha, C.R., l'honorable Roy Romanow, C.R., O.C., c.r., et l'honorable Aldéa Landry, C.R., C.M., c.r.

Tous les membres du Comité font partie du Conseil privé et sont nommés par le gouverneur en conseil après consultation entre le premier ministre et les chefs des partis de l'opposition.

Le Comité fournit au Parlement, et par son entremise aux Canadiens, l'assurance que le SCRS respecte la loi, les politiques et les institutions ministérielles dans l'exercice de ses fonctions. Il veille à ce que le Service ne sape pas les droits fondamentaux et les libertés des Canadiens. Le CSARS est le seul organisme indépendant, de l'extérieur, à être habilité par la loi et à avoir l'expertise voulue pour surveiller les activités du SCRS. De plus, il est la pierre angulaire de la tradition démocratique canadienne, car il assure la reddition de comptes de l'un des organismes gouvernementaux les plus puissants.

En plus d'assister aux réunions mensuelles du Comité, les membres président les audiences de plaintes, confient au personnel les études à mener et, en consultation avec lui, préparent les rapports de plaintes; ils visitent en outre les bureaux régionaux du SCRS, comparaissent devant le Parlement et exercent d'autres fonctions liées à leurs responsabilités.

Réunions et exposés
du CSARS, 2006-2007

5 avril 2006 : Le président prononce une allocution devant l'organisme Associatés, de l'école des affaires I.H. Asper de l'Université du Manitoba, à Winnipeg.

1^{er} mai 2006 : Le directeur exécutif associé et l'avocat principal rencontrent une délégation du Parlement

tchèque.

12 mai 2006 : Le président et le directeur exécutif font un exposé aux juges de la Cour fédérale au sujet des études du CSARS sur les mandats.

8 juin 2006 : Le directeur exécutif associé et des chercheurs supérieurs assistent au troisième Forum des organismes de surveillance tenu par l'inspecteur général du SCRS. Au nombre des participants figurent des représentants du commissaire du Centre de la sécurité des télécommunications, du Bureau de l'inspecteur général du SCRS et de la Commission des plaintes du public contre la GRC.

19 septembre 2006 : Le directeur exécutif, le directeur exécutif associé et l'avocat principal rencontrent le commissaire des Services de renseignement du Royaume-Uni, sir Peter Gibson, son adjoint David Massam et un représentant du Haut-commissariat du Royaume-Uni.

22 septembre 2006 : Le président prononce une allocution au Global Business Forum tenu à Banff, en Alberta.

26 septembre 2006 : Le directeur exécutif, le directeur exécutif associé et l'avocat principal rencontrent une délégation d'un comité parlementaire norvégien.

Suite à la page suivante

Section 3

Au sujet du CSARS

Dans son rapport annuel de 2005-2006, le CSARS a fait état de l'étude que le SCRS avait menée, sur le processus des mandats, par suite d'un moratoire imposé par le directeur après que la Cour fédérale eut rejeté une demande de mandat²². Pendant ce moratoire, qui s'est échelonné du 22 juin 2005 au 28 juin 2006, le directeur et l'avocat général du Service ont approuvé 38 mandats à titre exceptionnel. Par suite d'une évaluation du processus des mandats échelonnée sur un an, le SCRS a mentionné au CSARS que, pour l'étude des mandats, il était à mettre la dernière main à une approche simplifiée, dont l'entrée en vigueur est prévue pour la fin de 2007.

Au moment de rédiger le présent rapport, le CSARS a demandé au Service si la Cour fédérale lui avait demandé de modifier des demandes de mandat avant de les agréer. Trois cas lui ont été signalés.

²² Pour plus d'information sur le moratoire, voir « Mandats de la Cour fédérale : généralités et statistiques » dans la section 2 du Rapport annuel du CSARS 2005-2006.

Chaque année, le CSARS recueille des statistiques sur les demandes de mandats du Service et sur ceux que la Cour fédérale lui décerne en vertu des articles 12 et 16 de la Loi sur le SCRS. Le CSARS n'a pas les ressources voulues pour examiner tous les mandats octroyés au Service par la Cour fédérale, mais il en étudie un certain nombre dans le cadre de ses études annuelles.

Lorsque le CSARS examine un mandat, il se penche sur tous les éléments du processus pertinent, à commencer par l'élaboration de la demande. Il vérifie si :

- la demande de mandat reflète fidèlement l'information dont dispose le SCRS;
- les raisons fournies par le SCRS pour justifier les pouvoirs demandés sont raisonnables;
- le SCRS respecte les exigences applicables, sur le plan de la loi et des politiques, en demandant de se voir conférer des pouvoirs par la voie d'un mandat.

Le CSARS examine aussi le mandat même, décerné par la Cour fédérale, et l'usage des pouvoirs octroyés par la au Service (c.-à-d. la manière dont celui-ci exerce les pouvoirs conférés par le mandat).

Tableau 7
Statistiques sur les mandats

	2004-2005	2005-2006	2006-2007
Mandats nouveaux	40	24	42
Mandats remplacés ou renouvelés	207	203	134
Total	247	227	176*

* Comprend 25 mandats urgents.

En 2006-2007, la Cour fédérale a approuvé 42 mandats nouveaux, soit presque deux fois plus que pendant l'exercice précédent. Elle a toutefois approuvé le renouvellement ou le remplacement de 134 mandats seulement, ce qui représente une forte diminution par rapport aux 203 dont il est fait état pour l'exercice précédent. Pendant la même période, 42 mandats ont été suspendus ou ont pris fin sans être renouvelés. Aucune demande de mandat n'a été rejetée et la Cour fédérale a conféré au Service tous les pouvoirs ainsi sollicités.

DIRECTION DE L'ASIE, DE L'EUROPE ET DES AMÉRIQUES

Cette direction enquête sur les menaces qui émanent de la vaste zone dont elle a la charge, à savoir l'espionnage, le terrorisme (y compris l'extrémisme intérieur), les activités criminelles transnationales et celles qui sont influencées par l'étranger.

RÉGION INTERNATIONALE

La Région internationale (autrefois appelée Liaison avec l'étranger et Visites) gère la liaison du Service avec les organismes étrangers et coordonne les visites de représentants étrangers à l'Administration centrale et aux bureaux régionaux du SCRS. Elle a aussi charge de coordonner toutes les ententes conclues avec des organismes étrangers de renseignement de sécurité ou d'exécution de la loi en vertu du paragraphe 17(1), ainsi que le fonctionnement des postes d'agent à l'étranger.

Le Service mise sur ces missions à l'étranger pour aider à assurer la liaison avec les services étrangers de la sécurité et du renseignement et pour coordonner les visites de représentants étrangers à l'Administration centrale et dans les bureaux régionaux du SCRS. L'examen le plus récent de l'une de ces missions à l'étranger par le CSAARS est résumé dans son étude n° 2006-01, dans le rapport annuel de cette année.

MANDATS DE LA COUR FÉDÉRALE : GÉNÉRALITÉS ET STATISTIQUES

Mis à part leur caractère fort intrusif, les mandats sont l'un des instruments les plus puissants qui soient à la portée du SCRS. Ils lui procurent l'autorisation de la Cour fédérale à employer des méthodes d'enquête qui seraient autrement illégales, comme l'interception de communications téléphoniques. Pour cette raison, le recours aux mandats par le Service représente un important volet des études du CSAARS.

Dans le cadre de la réorganisation du SCRS, une nouvelle catégorie de postes a vu le jour, celle des agents à l'étranger (AE). Le terme générique agent à l'étranger englobe tout employé du SCRS qui travaille dans une mission à l'extérieur du Canada. Il peut comprendre les anciens agents de liaison-sécurité, les adjoints administratifs qui les appuient, les agents affectés temporairement dans une mission, les agents techniques affectés à une mission et ceux qui sont prêtés à l'étranger. Voici les fonctions des AE :

- gérer et recueillir des renseignements sur les menaces à la sécurité du Canada
- gérer et réunir des évaluations de sécurité à l'immigration
- assurer la liaison avec les gouvernements et organismes étrangers
- collaborer et partager l'information avec le personnel en poste dans les missions du Canada à l'étranger.

CENTRE INTÉGRÉ D'ÉVALUATION DES MENACES

Le Centre intégré d'évaluation des menaces (CIEM) produit des évaluations qui alertent le gouvernement à propos des menaces terroristes pesant sur le Canada et les intérêts canadiens à l'étranger. Une fois terminées, ces évaluations sont distribuées aux partenaires canadiens et étrangers. De plus, le CIEM est le pivot de la distribution des évaluations de la menace émanant de sesendants aux États-Unis, au Royaume-Uni, en Australie et en Nouvelle-Zélande²¹.

Au cours de la période à l'étude, le CIEM a effectué 83 évaluations de la menace et a redistribué 1 150 autres émanant de centres de fusion alliés. Au début de l'exercice financier, il a aussi commencé à publier *Coup d'œil sur les médias* à chaque jour ouvrable afin de le distribuer à ses clients. En outre, le CIEM a donné à ses clients canadiens 90 exposés sur l'évaluation de la menace. Plusieurs ministères en ont bénéficié, dont l'Agence du revenu du Canada et l'Agence des services frontaliers du Canada. Il est aussi à noter que le CIEM a effectué une évaluation de la menace à la demande du conseiller à la sécurité nationale. Dans son précédent rapport annuel, le CSARS a mentionné que l'effectif du CIEM n'était pas complet le 31 mars 2006. Le CIEM a fait savoir que son effectif était complet à pareille date en 2007.

2. Opérations

Depuis la réorganisation de mai 2006, chaque direction opérationnelle a charge d'enquêter sur toutes les menaces qui émanent de sa zone respectives, à l'exception de la Direction du terrorisme international qui se concentre exclusivement sur l'Al-Qaïda et sur les groupes dans sa mouvance, indépendamment des frontières géographiques.

DIRECTION DU TERRORISME INTERNATIONAL

Cette direction enquête dans le monde entier et au Canada, mettant l'accent sur les extrémistes islamistes qui se livrent à diverses activités liées au terrorisme et menaçant les Canadiens et les intérêts canadiens directement. Entre autres domaines d'intérêt notables de cette direction figure la radicalisation des islamistes au Canada.

DIRECTION DU MOYEN-ORIENT ET DE L'AFRIQUE

La Direction du Moyen-Orient et de l'Afrique concentre ses enquêtes sur les menaces qui émanent des pays du Moyen-Orient et de l'Afrique ou dont ces pays sont les principaux foyers. Cela englobe les questions du terrorisme, les activités influencées par l'étranger, la prolifération des armes de destruction massive et l'espionnage.

²¹ Pour plus d'information sur le CIEM, voir la section 1 du Rapport annuel du CSARS 2005-2006.

Nouveaux programmes

La Direction du filtrage de sécurité a pris part à trois programmes nouveaux :

1. Le Programme d'accès aux zones réglementées des infrastructures maritimes – vise à fournir des évaluations de sécurité pour assurer la sûreté des ports du Canada;
2. Le programme pour les voyageurs dignes de confiance – programme de prédé-douanement destiné aux voyageurs qui vont souvent aux États-Unis. Ce programme est en voie d'élaboration et aucune date n'est fixée pour son entrée en vigueur.
3. Protection des passagers – avec d'autres ministères, la Direction s'est employée à élaborer des programmes de contrôle des passagers de lignes aériennes, en particulier le programme intérieur des « personnes interdites de vol », entre en vigueur le 18 juin 2007.

DIRECTION DE L'ÉVALUATION DU RENSEIGNEMENT

La Direction de l'évaluation du renseignement (autrefois appelée Recherche, analyse et production) regroupe la fonction d'analyse clé du Service et en centralise les principaux mécanismes de transmission de renseignements. Elle élabore des analyses stratégiques et opérationnelles des menaces existantes et des problèmes nouveaux et produit des bulletins de renseignement, des évaluations de la menace et des risques, des études et des résumés des renseignements du SCRS.

Cette direction a aussi un rôle à jouer dans le processus d'inscription des entités terroristes. En vertu du *Code criminel*, le ministre de la Sécurité publique est tenu d'examiner la liste des entités terroristes tous les deux ans afin de déterminer s'il y a des motifs raisonnables d'y ajouter des entités ou d'en biffer certaines. Il fonde cette évaluation sur les rapports de renseignements de sécurité que prépare le SCRS. En 2006-2007, la Direction a élaboré deux rapports semblables. L'examen de la liste par le Ministère a été terminé et approuvé par le gouverneur en conseil le 9 novembre 2006.

DIRECTION DES SOURCES HUMAINES ET DU SOUTIEN AUX OPÉRATIONS

Cette direction assure un éventail de services de soutien et de coordination, dont la gestion des risques pour les activités opérationnelles à l'échelle du Service. Elle est le centre stratégique dans divers domaines, y compris la sécurité opérationnelle, les services multilingues et la gestion des sources humaines. Elle englobe aussi le Centre de gestion des menaces, qui assure le soutien au personnel opérationnel 7 jours par semaine, 24 heures par jour, à l'Administration centrale, aux bureaux régionaux et aux missions à l'étranger. De plus, elle coordonne la participation du Service aux grands événements tels les Jeux olympiques d'hiver qui se tiendront à Vancouver en 2010.

DIRECTION DES SERVICES TECHNIQUES ET SCIENTIFIQUES

Cette direction élabore et déploie des outils et mécanismes techniques afin de soutenir les opérations et enquêtes des autres directions du SCRS.

Comme c'était le cas lors des derniers exercices, les délais médians de remise de notes d'information ou d'avis de non-admissibilité par le Service ont en général été assez longs. Le délai médian de remise des notes d'information concernant les dossiers d'immigration a été de 460 jours civils pour les demandes présentées au Canada, de 620 jours pour celles provenant des États-Unis et de 161 jours pour celles provenant de l'étranger. Pour les notes d'information concernant les demandeurs de résidence permanente qui étaient des réfugiés au Canada, le délai de traitement médian a été de 442 jours et, pour les demandes relatives aux dossiers assujettis au Programme de contrôle de sécurité préliminaire, il a été de 365 jours. En ce qui touche les avis de non-admissibilité, le CSARS a relevé des délais médians semblables.

Le tableau 6 présente un aperçu triennal des délais médians du Service à fournir des avis de vérification de données.

Tableau 6
Délais médians (en jours) à fournir des avis de vérification de données

	2004-2005	2005-2006	2006-2007
Citoyenneté	1	1	1
Immigration (Canada) ¹⁹	44	70	78
Immigration (États-Unis) ²⁰	150	62	29
Demandes d'immigration, de l'étranger	7	16	14
Détermination du statut de réfugié	56	96	98
Contrôle de sécurité préliminaire	27	23	19

Autres activités de filtrage

En 2006-2007, la Direction du filtrage de sécurité a étudié 114 500 demandes de visa de ressortissants étrangers. Elle a en outre continué d'assurer le filtrage à l'égard de divers programmes d'accès à des sites. Pour plus d'information sur les activités de filtrage de sécurité de cette direction, voir l'étude n° 2006-07 du CSARS dans le rapport annuel de cette année.

¹⁹ Comprend certaines catégories de personnes qui demandent, au Canada, le statut de résident permanent.

²⁰ Comprend les personnes qui sont admises légalement au Canada depuis au moins un an et qui peuvent présenter leurs demandes aux bureaux de Citoyenneté et Immigration aux États-Unis.

En 2006-2007, la Direction a reçu 92 300 demandes dans le cadre de divers programmes de filtrage à l'immigration (voir le tableau 5). Le nombre de demandes reçues tant du Canada que de l'extérieur et celui des demandes de filtrage de candidats au statut de réfugié et de contrôle de sécurité préliminaire sont demeurés à peu près les mêmes que pour l'exercice précédent.

Tableau 5
Filtrage de sécurité à l'immigration

	Demandes*						Avis
	2004-2005	2005-2006	2006-2007	2004-2005	2005-2006	2006-2007	
Présentées au Canada et à l'étranger ¹⁶	56 100	63 200	62 800	88	133	201	
Contrôle de sécurité préliminaire ¹⁷	22 900	17 100	17 900	184	89	143	
Détermination du statut de réfugié ¹⁸	14 200	11 700	11 600	110	127	153	
Total partiel	93 200	92 000	92 300	382	349	497	
Demandes de citoyenneté	161 200	308 000	227 300	124	120	155	
Total	254 400	400 000	319 600	506	469	652	

* Chiffres arrondis à la centaine la plus proche.

Le SCRS ne trouve aucun renseignement défavorable dans la grande majorité de ses enquêtes de filtrage de candidats au statut de réfugié, à l'immigration ou à la citoyenneté. En 2006-2007, il a présenté 157 notes d'information, 44 avis de non-admissibilité et 2 lettres d'anecdote à l'égard de dossiers d'immigration.

¹⁶ Comprend les demandes de résidents permanents au Canada et à l'étranger (à l'exclusion du Programme de détermination du statut de réfugié), de résidents permanents aux États-Unis et de demandeurs à l'étranger.

¹⁷ Dans le cas des personnes qui se présentent à la frontière canadienne ou à d'autres point d'entrée et demandent le statut de réfugié.

¹⁸ Les réfugiés, au sens de la LIR, qui présentent au Canada une demande de statut de résident permanent.

Les avis du SCRS concernant le filtrage de sécurité peuvent prendre l'une ou l'autre des cinq formes suivantes :

1. **Avis de vérification de données** : remis dans les cas de filtrage pour le gouvernement et l'immigration si le Service ne trouve aucun renseignement défavorable au sujet du demandeur.
2. **Lettre d'anecdote** : fournie à Citoyenneté et Immigration Canada (CIC) et à l'Agence des services frontaliers du Canada (ASFC) si le Service a des renseignements au sujet d'un demandeur qui prend ou a pris part à des activités étrangères à la sécurité, décrites dans la Loi sur l'immigration et la protection des réfugiés (LIPR).

3. **Note d'information** : remise dans les cas de filtrage pour le gouvernement si le SCRS a des informations qui pourraient influencer la décision de l'organisme demandeur d'octroyer à un candidat une habilitation de sécurité ou d'accès à des sites. Aussi remise dans les cas de filtrage à l'immigration si le Service a des informations voulant que le candidat trempe ou ait trempé dans des activités qui ne le rendent pas nécessairement interdit de territoire au Canada.

4. **Avis de non-admissibilité** : fourni à l'ASFC si le demandeur est réputé interdit de territoire au Canada, selon les dispositions de la LIPR relatives à la sécurité.
5. **Avis de refus** : remis dans les cas où le Service recommande à un organisme demandeur de refuser une habilitation de sécurité ou d'accès à des sites au candidat.

Le **Filtrage à l'immigration** amène la Direction du filtrage de sécurité à effectuer des enquêtes et à conseiller Citoyenneté et Immigration Canada et l'Agence des services frontaliers du Canada pour appuyer le traitement des demandes de candidats au statut de réfugié ainsi qu'à l'immigration et à la citoyenneté. À cet égard, le Service tient ses pouvoirs du paragraphe 34(1) de la Loi sur l'immigration et la protection des réfugiés.

Le Service ne décide pas qui se voit octroyer une habilitation de sécurité. Au ministère ou organisme demandeur, il fait plutôt part des renseignements qui pourraient influencer sur la décision de celui-ci d'en octroyer une ou pas. Rares sont les occasions où le SCRS lui recommande de refuser l'habilitation. Il incombe toutefois au demandeur d'accepter ou de rejeter cette recommandation. En 2006-2007, le Service a présenté 14 notes d'information contenant des renseignements défavorables. Il n'a remis aucun avis de refus.

Le SCRS offre aussi un service de filtrage pour l'accès à des sites. Contrairement à la core de sécurité du gouvernement, l'autorisation d'accès permet simplement au titulaire d'entrer dans certaines zones protégées d'immuables ou elle l'accrédite en vue d'un événement spécial. En 2006-2007, le SCRS a reçu plus de 83 900 demandes de filtrage de ce type et il a remis trois notes d'information aux organismes demandeurs. L'augmentation, de quelque 69 p. 100, des demandes d'accès aux centrales nucléaires est l'aboutissement d'un cycle quinquennal de renouvellement des habilitations existantes.

Il n'y a eu aucun événement spécial pour lequel le Service a fourni des évaluations. Le nombre de demandes d'autorisation d'accès à tous les autres sites est demeuré à peu près identique à celui des exercices précédents.

Tableau 4
Filtrage concernant l'accès à des sites*

	2004-2005	2005-2006	2006-2007
Cité parlementaire	1 100	1 000	1 100
Zones réglementées d'aéroports	31 100	37 600	39 300
Centrales nucléaires	6 800	10 600	17 900
Agence des services frontaliers du Canada (ASFC)/ Expéditions rapides et sécuritaires (EXPRES) ¹³	21 500	3 100	23 100
Accréditation en vue d'événements spéciaux	1 800	5 600	0
Autres ministères	2 300	2 400	2 500
Total	64 600	60 300	83 900

* Chiffres arrondis à la centaine la plus proche.

¹³ Le programme EXPRES est entré en vigueur en 2004-2005. Les données de 2006-2007 représentent les demandes de filtrage à la fois pour EXPRES et pour l'ASFC, et le SCRS les comptabilise maintenant ensemble.

Tableau 2
Filtrage de sécurité du SCRS pour le gouvernement*

	2004-2005	2005-2006	2006-2007
Demandes du MDN	9 100	9 200	13 100
Demandes d'autres ministères ou organismes	27 400	32 900	38 100
Total	36 500	42 100	51 200
Evaluations fournies au MDN	9 000	8 900	13 100
Evaluations fournies aux autres ministères ou organismes ¹⁴	27 600	28 900	41 800
Total	36 600	37 800	55 000

* Chiffres arrondis à la centaine la plus proche.

Pour jauger son efficacité à répondre aux demandes de filtrage de sécurité, le SCRS calcule les délais d'exécution en nombres médians de jours. Comme le montre le tableau 3, les délais médians ont augmenté dans tous les cas, sauf un, par rapport à l'exercice précédent. Le délai d'exécution d'une habilitation de niveau I a plus que doublé pour les ministères autres que le MDN.

Tableau 3
Délais médians (en jours civils)

	2004-2005	2005-2006	2006-2007
MDN	Niveau I (Confidentiel)	49	24
	Niveau II (Secret)	63	19
	Niveau III (Très secret)	70	39
Autres que le MDN	Niveau I (Confidentiel)	12	15
	Niveau II (Secret)	14	13
	Niveau III (Très secret)	69	60

¹⁴ Comprend les évaluations effectuées pour les gouvernements provinciaux et pour l'accès aux centrales nucléaires.

1. Renseignement

Voici un exposé des fonctions de ces groupes.

- 1. le **Renseignement**, qui compte cinq directions : a) Filtrage de sécurité, b) Évaluation du renseignement, c) Sources humaines et soutien aux opérations, d) Services techniques et scientifiques, et e) Centre intégré d'évaluation des menaces;
- 2. les **Opérations**, composées de trois directions et d'un bureau régional : a) Terrorisme international, b) Moyen-Orient et Afrique, c) Asie, Europe et Amériques, et d) Région internationale;
- 3. les **Régions**, au nombre de six.

DIRECTION DU FILTRAGE DE SÉCURITÉ

L'une des plus grandes directions du SCRS, celle du filtrage de sécurité, comporte deux volets centraux touchant l'un le gouvernement et l'autre, l'immigration.

Le **filtrage pour le gouvernement** porte sur les enquêtes de sécurité de tous les fonctionnaires¹³ qui, dans le cadre de leurs fonctions, doivent avoir accès à des renseignements ou à des biens classifiés. Les résultats de ces enquêtes sont des évaluations de sécurité qui servent à jauger la loyauté des intéressés envers le Canada quant à leur fiabilité personnelle et qui sont fournies au ministre ou à l'organisme demandeur. Depuis toujours, les clients qui recourent le plus à ce service sont Travaux publics et Services gouvernementaux Canada et le ministre de la Défense nationale (MDN), qui regroupent respectivement 28 et 26 p. 100 de routes les demandes en 2006-2007.

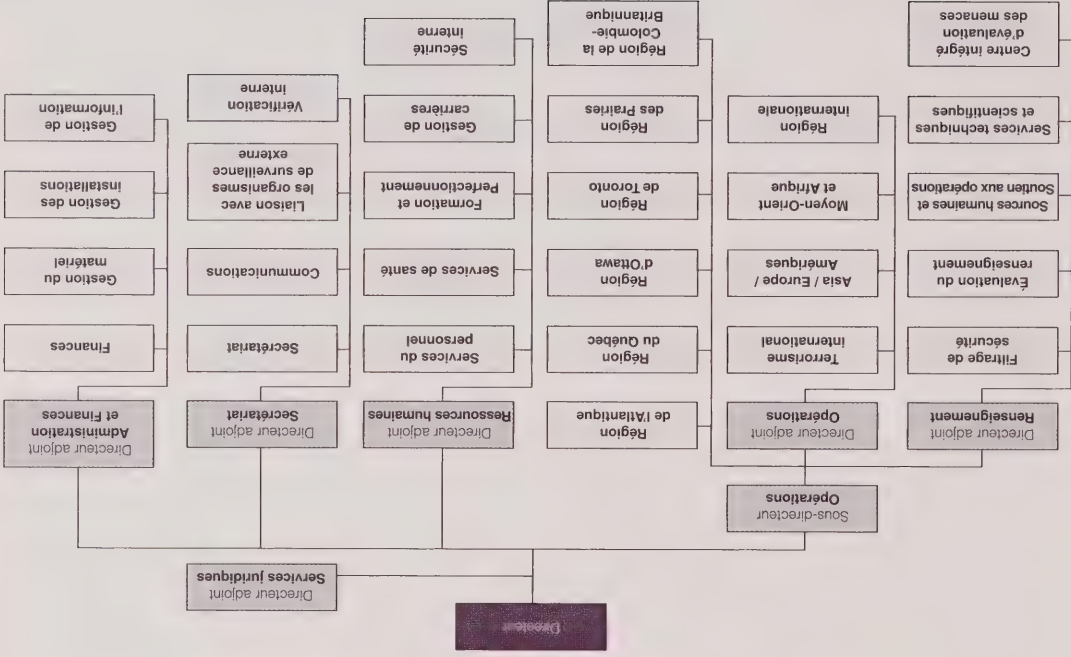
Comme le montre le tableau 2, le SCRS a reçu 51 200 demandes d'habilitations de sécurité nouvelles ou mises à jour en 2006-2007 et il a fourni 55 000 évaluations de sécurité aux ministères fédéraux. Le nombre des demandes a augmenté de quelque 22 p. 100 par rapport à l'exercice précédent et celui des évaluations de sécurité fournies par le SCRS a crû de 46 p. 100 comparativement aux exercices antérieurs.

¹³ Le SCRS ne fait pas d'enquêtes de sécurité au nom de la police nationale du Canada. La GRC s'en occupe elle-même.

D. Activités opérationnelles du SCRS

En mai 2006, le SCRS a instauré une nouvelle structure opérationnelle. Cette réorganisation de ses ressources visait, selon lui, à pouvoir accroître sa capacité opérationnelle, intégrer et améliorer ses services d'analyse et de production et relever le soutien général. Le sous-directeur, Opérations, qui relève du directeur du SCRS, a désormais chargé de trois groupes :

Service canadien du renseignement de sécurité



- veiller à ce que le matériel technique et les systèmes d'information du SCRS répondent aux besoins de ses enquêtes.

INSTRUCTIONS MINISTÉRIELLES

En vertu du paragraphe 6(2) de la *Loi sur le SCRS*, le ministre de la Sécurité publique peut donner des instructions écrites afin de guider les activités et enquêtes du SCRS. Ses dernières instructions remontent à 2001, année où un recueil a été remis au CSARS. En juin 2007, cependant, celui-ci a reçu les *Exigences nationales en matière de renseignement de sécurité* pour 2006-2008 (il n'y en avait pas eu pour 2005-2006).

MODIFICATIONS À LA POLITIQUE OPÉRATIONNELLE DU SCRS

Les politiques administratives et opérationnelles du SCRS et celles qui ont trait à la sécurité et aux ressources humaines comportent des règles et des procédures qui régissent l'ensemble des activités du Service. Les politiques administratives et celles relatives à la sécurité et aux ressources humaines sont toutes des politiques internes. Les politiques opérationnelles, qui décrivent la manière dont les employés du SCRS doivent exercer leurs fonctions, sont mises à jour régulièrement selon la politique gouvernementale et les modifications d'ordre législatif et autre. Le CSARS les examine pour s'assurer qu'elles respectent la *Loi sur le SCRS* et les instructions ministérielles.

En 2006-2007, le SCRS a révisé et/ou publié plus de 120 politiques. Certaines révisions étaient d'ordre administratif et les autres, d'ordre opérationnel, avaient trait à l'obtention de mandats et à l'approbation d'enquêtes relevant des articles 12 et 16. Aucune politique n'a été élaborée dans le cadre de la réorganisation du SCRS, mais on en a modifié 14 d'ordre général et 77 d'ordre opérationnel (voir *Activités opérationnelles du SCRS*).

L'un des projets stratégiques que le Service a entrepris en 2006-2007, appelé projet de délégation des responsabilités, émanait du directeur. C'est une étude des diverses politiques opérationnelles qui visait à déterminer les cas où il fallait déléguer les responsabilités de direction et de gestion. Le SCRS a informé le CSARS que ce projet suit son cours et qu'il en partagera les résultats une fois qu'il sera terminé.

RÈGLEMENTS ET NOMINATIONS PAR LE GOUVERNEUR EN CONSEIL

Selon le paragraphe 8(4) de la *Loi sur le SCRS*, le gouverneur en conseil peut établir, pour le Service, des règlements visant les pouvoirs et fonctions de son directeur ainsi que la conduite et la discipline de ses employés.

Le gouverneur en conseil n'a pris aucun règlement semblable en 2006-2007.

EXIGENCES NATIONALES EN MATIÈRE DE RENSEIGNEMENT DE SÉCURITÉ

Le ministre de la Sécurité publique donne des instructions, intitulées « Exigences nationales en matière de renseignement de sécurité », qui exposent les orientations générales du gouvernement quant aux plans sur lesquels le Service doit faire porter ses efforts d'enquête et qui le guident dans l'exercice de ses responsabilités en matière de collecte, d'analyse et de conseil.

Les Exigences nationales de 2006-2008 enjoignent au Service de maintenir une capacité souple à répondre aux besoins de renseignements de sécurité qui se dessinent au Canada en tablant sur la gestion des risques. Le Ministre note que le contexte actuel de la menace a un caractère de plus en plus international et transnational, nombre des menaces à la sécurité du Canada qui émanent de l'extérieur du pays, requérant des enquêtes à l'étranger. Le SCRS est donc invité à poursuivre ses enquêtes sur les menaces à la sécurité nationale tant au Canada même que dans d'autres pays.

Pour 2006-2008, le Ministre a prescrit au SCRS de s'attacher aux priorités qui suivent en matière de renseignements de sécurité :

- protéger contre la possibilité qu'une attaque terroriste survienne au Canada ou y prenne naissance ou qu'une telle attaque affecte des citoyens ou des biens canadiens à l'étranger, et conseiller le gouvernement à ce sujet;
- poursuivre les recherches et analyses appuyant l'inscription des entités terroristes en vertu du *Code criminel* du Canada et lutter contre le financement du terrorisme;
- soutenir les efforts du gouvernement du Canada en Afghanistan;
- collaborer de façon étroite avec les autres ministères dans la lutte aux activités criminelles transnationales;
- enquêter sur les menaces à la sécurité du Canada qui découlent d'activités de pays qui se livrent à l'espionnage;
- poursuivre l'identification des pays et des groupes – et les enquêtes à leur sujet – qui possèdent des armes de destruction massive ou peuvent tenter d'en acquérir, et conseiller le gouvernement au sujet des menaces que constituent ces activités;
- appuyer la collecte de renseignements étrangers au Canada afin de prêter assistance au ministre des Affaires étrangères et/ou au ministre de la Défense nationale en vertu de l'article 16 de la *Loi sur le SCRS*;
- exécuter les programmes de filtrage de sécurité pour les ministères et organismes fédéraux et pour d'autres clients;
- fournir au gouvernement du Canada des évaluations du renseignement et veiller à ce que le SCRS se tienne au fait des circonstances politiques, sociales et économiques qui peuvent susciter des menaces à la sécurité du Canada;

À l'occasion, le Service doit modifier des ententes avec des organismes étrangers afin de tenir compte de changements subis par un partenaire étranger¹², de relancer une entente inappliquée ou de placer une entente à l'état latent. Huit ententes ont été modifiées au cours de l'exercice à l'étude. Huit autres ont été restituées.

Le directeur du SCRS a le pouvoir discrétionnaire d'approuver l'élargissement ou la modification d'une entente avec un organisme étranger sans devoir obtenir l'autorisation du Ministre. Ces ententes demeurent assujetties aux mises en garde ou aux instructions ministérielles qui peuvent avoir été formulées lors de leur approbation initiale.

Le CSARS examine toutes les ententes avec des organismes étrangers, tant nouvelles que réhaussées ou modifiées, tel que prescrit au sous-aligné 38a)(iii) de la *Loi sur le SCRS*. À cette fin, il vérifie :

- si les ententes conclues par le SCRS avec des organismes étrangers respectent les conditions énoncées dans la *Loi sur le SCRS*, les instructions ministérielles et la politique opérationnelle;
- si l'approbation du ministre de la Sécurité publique et du directeur du SCRS a été donnée lorsque le Service commence à échanger des informations;
- si l'on tient compte du bilan du pays hôte de l'organisme étranger en matière de droits de la personne;
- si le dernier profil de l'entente est conforme aux lignes directrices du SCRS.

En 2006-2007, le CSARS a examiné 19 ententes conclues avec des organismes étrangers de 14 pays. Il a constaté que toutes ces ententes étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et aux politiques opérationnelles.

Le CSARS a aussi constaté que le Service s'était enquis de la situation des droits de la personne dans tous les pays et organismes en question. De plus, le Service avait usé de prudence dans ses échanges d'information avec des pays au bilan douteux en matière de droits de la personne.

Le CSARS a aussi observé une amélioration dans la présentation à point nommé des profils d'ententes. Tous les profils examinés reflétaient les circonstances politiques actuelles des pays et organismes en question ainsi que celles en matière de sécurité et de droits

¹² Ces changements peuvent englober la fusion de deux organismes ou un changement de nom d'un organisme.

B. Ententes avec des organismes canadiens et étrangers

Les articles 13 et 17 de la *Loi sur le SCRS* habiliteront le Service à conclure des ententes avec des organisations ou des organismes canadiens et étrangers dans l'exercice de ses fonctions. Le CSAARS reçoit copie de ces ententes à leur entrée en vigueur et il en examine un échantillon chaque année.

ENTENTES AVEC DES ORGANISMES CANADIENS

Le SCRS collabore souvent avec des ministères et organismes fédéraux, des gouvernements provinciaux et des organismes de maintien de l'ordre. Depuis le 1^{er} septembre, des groupes plus nombreux s'occupent de sécurité nationale, dont les forces de police et d'autres partenaires du secteur public. Cela représente un défi pour le Service, car il doit cultiver de saines relations avec tous ses partenaires, tant anciens que nouveaux, pour s'assurer de l'efficacité à la fois des échanges d'information et de la conduite des opérations conjointes.

Nombre d'accords conclus avec des organismes canadiens prennent la forme de protocoles d'entente, mais le SCRS peut collaborer avec eux même si aucun protocole d'entente n'a été conclu. Le 31 mars 2007, il en avait conclu 35 avec des partenaires canadiens : 19 avec des ministères ou organismes fédéraux et 16 avec des entités provinciales et municipales.

En septembre 2006, le Service a mis à jour son protocole d'entente avec la GRC. Le protocole révisé reflète de nouveaux mécanismes de coopération et de consultation entre les deux organismes. Il souligne en outre la mise en œuvre d'une stratégie nationale de lutte contre le terrorisme pour faciliter la coopération et la coordination du SCRS et de la GRC. De plus, il établit des priorités communes aux deux organismes, en ce qui touche la vue d'ensemble de la menace et les enquêtes antiterroristes, ainsi que l'élaboration de programmes de formation conjoints.

ENTENTES AVEC DES ORGANISMES ÉTRANGERS

Le 31 mars 2007, le SCRS avait conclu 271 ententes avec des organismes de 147 pays. Toute nouvelle entente semblable doit être approuvée par le ministre de la Sécurité publique, en consultation avec son homologue des Affaires étrangères. Même en l'absence d'une telle entente, le SCRS peut quand même accepter les informations que lui fournissent spontanément les organismes ou organisations de pays étrangers. Le Ministère a approuvé sept ententes nouvelles en 2006-2007 et il en a élargi six qui existaient déjà.

AGISSEMENTS ILLICITES DU SCRS

En vertu du paragraphe 20(2) de la *Loi sur le SCRS*, le directeur du Service doit présenter un rapport au Ministre s'il estime qu'un employé du Service peut avoir commis un acte illicite dans l'exercice de ses fonctions. Le cas échéant, le Ministre doit alors transmettre ce rapport au procureur général du Canada et au Comité, accompagné de ses observations. En 2006-2007, aucun employé du SCRS n'a commis d'acte illicite et aucun rapport semblable n'a été présenté.

COMMUNICATION D'INFORMATIONS

L'article 19 de la *Loi sur le SCRS* interdit la communication d'informations obtenues par le Service dans le cadre d'enquêtes, sauf dans des circonstances particulières. Ainsi, selon la *Loi*, le SCRS peut communiquer des informations :

1. pouvant servir dans le cadre d'une enquête ou de poursuites relatives à une infraction présumée à une loi fédérale ou provinciale, et cela, aux agents de la paix compétents pour mener l'enquête, au ministre de la Sécurité publique et au procureur général de la province concernée;
2. concernant la conduite des affaires étrangères du Canada, et cela, au ministre des Affaires étrangères;
3. concernant la défense du Canada, et cela, au ministre de la Défense nationale;
4. essentielles pour des raisons d'intérêt public, selon le Ministre, et cela, à un ministre ou à un fonctionnaire fédéral.

Il importe de noter que l'alinéa 19(2)d) habilite le ministre de la Sécurité publique à passer des informations réputées être dans l'intérêt national ou public. Si de telles informations sont divulguées, le directeur du SCRS doit en faire rapport au CSARS. Cela est extrêmement rare : il n'y a eu que deux cas de communications visées par cet alinéa.

Le Service peut aussi communiquer des informations, par écrit ou verbalement, aux organismes d'exécution de la loi ou aux entités fédérales, tels que le ministre de la Défense nationale et Affaires étrangères Canada. Lorsque le SCRS autorise la GRC à utiliser ses informations dans des instances judiciaires, il doit le faire par écrit.

Le Service a présenté plus de 130 notes de communication au cours de l'exercice 2006-2007.

L'IG a mentionné que le nombre d'incidents de non-conformité à la politique opérationnelle avait augmenté en 2005-2006. Voici comment elle définit non-conformité : toute action qui ne respecte pas les règles, procédures, principes et lignes directrices énoncées dans la politique opérationnelle. Elle ne fait pas de distinction quant à l'importance relative des cas de non-conformité.

L'une des préoccupations exprimées par l'IG était que l'énoncé annuel d'orientations du SCRS pour 2005 reposait sur les exigences nationales en matière de renseignement de sécurité, données au SCRS par un comité spécial du Cabinet. Selon l'IG, les exigences nationales deviennent un document confidentiel du Cabinet et limitent ainsi l'accès de l'IG à l'ensemble de l'information du SCRS.

L'IG a relevé plusieurs cas où l'information avait été traitée sans précaution, dont certains où son personnel a trouvé des divergences et des inexactitudes dans les dossiers du SCRS et d'autres où celui-ci n'a pu localiser ou repérer les documents demandés.

L'IG a relevé plusieurs failles dans la politique actuelle du SCRS. Elle a noté que le cadre stratégique ne reflétait pas la procédure actuelle pour l'approbation des échanges d'information avec les organismes partenaires. L'IG a fait état de l'élargissement du fossé entre la politique et la pratique dans l'exercice des pouvoirs conférés par la voie de mandats.

En vertu de l'article 16 de la *Loi sur le SCRS*, le Service est tenu de limiter au Canada la collecte de renseignements étrangers, tandis que les renseignements de sécurité recueillis en vertu de l'article 12 peuvent l'être au Canada et à l'étranger¹¹. Dans son certificat de 2006, l'IG fait état d'un chevauchement considérable des enquêtes menées par le Service en vertu des articles 12 et 16, ce qui l'a amenée à conclure que, dans certains cas, la portée de la restriction géographique de l'article 16 est nulle.

En conclusion, l'IG a affirmé avoir relevé une lacune dans les politiques opérationnelles régissant certaines opérations du SCRS à l'étranger.

Pour plus d'information, prière de vous reporter à la page d'accueil du Bureau de l'inspecteur général, sur le site Web de la Sécurité publique (securitepublique.gc.ca).

¹¹ Voir les détails au sujet d'une activité visée à l'article 16, dans l'étude n° 2006-04 du CSARS.

Dans son rapport, le directeur a aussi noté que le Service avait continué d'enquêter sur les tentatives de pays étrangers pour faire de l'espionnage, avoir accès à des techniques exclusives et multiplier les armes de destruction massive. Trois pays étaient considérés comme prioritaires en 2005-2006, mais beaucoup d'autres se livraient à des activités semblables.

Dans son rapport annuel de 2005-2006, le CSARS a déjà fait état des statistiques sur le filtrage de sécurité dont fait rapport le directeur. Celui-ci a noté que le SCRS avait élargi ses responsabilités en matière de filtrage de sécurité en signant des ententes avec deux provinces et qu'il avait assumé de nouvelles obligations en vertu de l'accord tripartite de 2005 intitulé Partenariat nord-américain pour la sécurité et la prospérité.

Le directeur a noté que le SCRS avait étendu son réseau de coopération avec ses partenaires canadiens par deux nouveaux protocoles d'entente, en 2005-2006. Il a aussi mentionné que le SCRS entretenait d'excellentes relations avec ses principaux partenaires étrangers. Il a aussi mis l'accent sur la manière dont le Service exerce une diligence raisonnable à l'égard du bilan des pays et organismes partenaires, en matière de droits de la personne, et sur le fait qu'il continue de donner aux nouveaux services de renseignement une formation sur les principes de la collecte des renseignements en démocratie.

Le lecteur est prié de noter que le SCRS affiche des rapports publics non classifiés sur son site Web (www.csis-scrs.gc.ca).

CERTIFICAT DE L'INSPECTEUR GÉNÉRAL DU SCRS (2006)

Le poste d'inspecteur général (IG) a été créé en 1984 en vertu de la *Loi sur le SCRS*. Son titulaire effectue des études internes du SCRS au nom du ministre de la Sécurité publique, scrutant les opérations du Service et fournissant l'assurance que celui-ci respecte la *Loi sur le SCRS*, les instructions ministérielles et la politique opérationnelle.

Chaque année, l'IG présente au Ministre un certificat attestant de la mesure où il est satisfait du rapport annuel du directeur du SCRS. Dans ce certificat, il l'informe en outre de tout cas où le SCRS aurait négligé de se conformer à la *Loi* ou aux instructions ministérielles et où il aurait exercé ses pouvoirs de façon abusive ou inutile.

L'IG s'est dit satisfait du rapport annuel du directeur du SCRS pour 2005-2006, mais elle a noté des écarts entre les statistiques dont il est fait état et les faits qu'on lui avait fournis. L'IG a conclu que le Service n'avait pas outrepassé les pouvoirs que lui confère la loi et qu'il avait exercé ses fonctions de façon efficace et professionnelle.

Mécanismes redditionnels du SCRS

A. Exigences en matière de rapports

RAPPORT ANNUEL DU DIRECTEUR DU SCRS (2005-2006)

Chaque année, le directeur du SCRS doit présenter au ministre de la Sécurité publique un rapport classifié décrivant en détail les priorités et les activités opérationnelles du Service. De plus, selon la *Loi sur le SCRS*, l'inspecteur général du Service est tenu d'examiner ce rapport et de faire parvenir au Ministre un certificat attestant de la mesure où il est satisfait de son contenu. Enfin, le Ministre transmet copie des deux documents au CSARS afin qu'il les examine, tel que prescrit à l'alinéa 38a) de la *Loi sur le SCRS*.

Les priorités centrales du Service sont d'assurer la sécurité du public et de protéger les infrastructures essentielles clés. Le directeur s'est dit favorable à une loi appropriée sur l'accès autorisé afin de mieux permettre au SCRS de faire face à ces priorités. À son avis, une telle loi accroitrait la capacité du SCRS à recueillir des renseignements et lui faciliterait l'accès aux réseaux de télécommunication modernes.

La tenue d'enquêtes sur le terrorisme et les menaces terroristes contre le Canada et les intérêts canadiens à l'étranger demeurent la toute première priorité opérationnelle du Service, en particulier, les nombreuses menaces que représente l'extrémisme islamique. Le directeur a souligné que la menace d'Al-Qaïda était très grave à l'étranger et que nombre des cibles du Service (y compris quelques citoyens canadiens) sont impliquées dans des groupes terroristes internationaux dont les activités menacent directement des intérêts canadiens à l'étranger.

Le Service a continué d'élargir son rôle de soutien des Forces canadiennes à l'étranger. En 2005-2006, il a ainsi appuyé les Forces canadiennes en Afghanistan, participé à la mission visant à reprendre des otages canadiens en Iraq et aidé à l'évacuation de citoyens canadiens du Liban. Le directeur a fait état publiquement de ces activités en octobre 2006.

De plus, le directeur a mentionné que le SCRS menait des enquêtes sur de nombreuses activités intérieures liées au terrorisme, dont la menace de violence grave émanant de l'extrémisme autochtone et des mouvements militant pour le nationalisme québécois, pour la suprématie blanche et pour l'environnement. Pour la deuxième année, le directeur a souligné la menace que représentent au Canada les extrémistes d'origine intérieure dans la mouvance d'Al-Qaïda, faisant état des poursuites criminelles entamées contre 15 personnes de Toronto, par exemple.

Section 2

Mécanismes additionnels du SCRS

Retard allégué à traiter une demande de citoyenneté

Rapport n° 2006-05

Le CSARS a fait rapport au sujet d'une autre plainte, présentée en vertu de l'article 41 de la *Loi sur le SCRS*, dans laquelle il était allégué que le SCRS aurait causé de façon délibérée et répréhensible un retard dans le traitement de la demande de citoyenneté du plaignant. Celui-ci, un résident permanent du Canada, avait demandé la citoyenneté canadienne et avait subi une entrevue de filtrage de sécurité de la part du Service, à la demande de Citoyenneté et Immigration Canada¹⁰.

Dans cette affaire, le SCRS a expliqué au CSARS que le retard de l'enquêteur à présenter le rapport de l'entrevue du plaignant était en partie attribuable aux problèmes de la Direction du filtrage de sécurité, quant à sa charge de travail dans la foulée du 11 septembre.

Les pouvoirs conférés au CSARS à l'article 41 de la *Loi sur le SCRS* n'englobent pas les études sur Citoyenneté et Immigration Canada (CIC). Le CSARS n'a donc pas pu établir le rôle joué par CIC dans un retard à traiter la demande de citoyenneté du plaignant. En ce qui touche le rôle du Service, le CSARS a constaté que celui-ci :

- avait tardé à fixer l'entrevue entre le plaignant et l'enquêteur chargé du filtrage;
- avait tardé à terminer et à présenter le rapport d'entrevue;
- avait contribué à des retards supplémentaires en recommandant à CIC de consulter un autre organisme fédéral.

Le CSARS a conclu que ces retards étaient imprévisibles, bien que regrettables, et que les allégations du plaignant n'étaient pas corroborées.

¹⁰ Selon l'article 14 de la *Loi sur le SCRS*, le Service peut fournir des conseils à un ministre sur les questions de sécurité du Canada, ou lui transmettre des informations sur des questions de sécurité ou des activités criminelles.

Prétendues fausses déclarations

Rapport n° 2006-04

Le CSARS a fait rapport d'une décision à l'égard d'une plainte présentée en vertu de l'article 41 de la *Loi sur le SCRS*. Le plaignant, Human Concern International (HCI), alléguait que le Service avait fait une fausse déclaration à la Cour fédérale du Canada, par l'entremise des ministres de la Sécurité publique et de l'Immigration. Il alléguait en outre qu'un document déposé par les deux ministres était fondé sur des renseignements du SCRS qui, celui-ci le savait ou aurait dû le savoir, nuisaient au caractère, à la réputation et à la qualité de l'organisme plaignant. De surcroît, celui-ci a soutenu que, n'étant pas partie au procès, il n'avait pas eu officiellement l'occasion de contester une déclaration du Service qui avait été publiée par la suite dans deux journaux canadiens.

Lorsqu'il a reçu cette plainte, le CSARS a incité les deux parties à chercher une solution de rechange à ce différend. Les discussions à cet égard ayant échoué, le CSARS a mené sa propre enquête. Il a conclu que le Service avait fait une allégation non corroborée au sujet du plaignant, dans l'opinion qu'il avait formulée aux ministres de la Sécurité publique et de l'Immigration et qui avait par la suite été présentée à la Cour fédérale. De plus, le CSARS a conclu que le SCRS savait que les ministres de la Sécurité publique et de l'Immigration, tout comme la Cour fédérale, prêteraient foi à son opinion. Pour cette raison et puisque HCI n'avait pas la possibilité de répondre à la déclaration contestée, le SCRS aurait dû veiller à éviter de faire une déclaration non corroborée qui pouvait causer un préjudice au plaignant ou lui faire perdre des appuis et son financement.

Recommandations

Le CSARS a recommandé :

- que le SCRS rétracte officiellement cette déclaration particulière, et ce, en informant le ministre de la Citoyenneté et de l'Immigration, le ministre de la Sécurité publique, la Cour fédérale du Canada et les éditeurs des deux journaux.
- que le SCRS s'excuse auprès de HCI d'avoir fait une déclaration non corroborée.

Le CSARS a conclu qu'il existait des motifs raisonnables de croire que le plaigiant :

- pouvait avoir fraye sciemment avec des personnes considérées comme une menace à la sécurité;
 - avait omis de signaler au SCRS ses soupçons avoués au sujet des activités de ces personnes; pouvait avoir révélé des renseignements classifiés, ce qui était une infraction à la sécurité.
- Le CSARS a conclu que le directeur avait des motifs raisonnables de révoquer l'habilitation de sécurité du plaigiant.

Recommandations

Le CSARS a recommandé que le SCRS :

- élabore et mette en œuvre une politique prescrivant que ses employés soient informés de leur droit à être représentés par un avocat et qu'ils aient la possibilité d'en consulter un avant et pendant une entrevue menée dans le cadre d'une enquête sur une infraction à la sécurité ou sur un écart de conduite;
- dresse un répertoire des avocats du secteur privé qui sont titulaires d'une core de sécurité « Très secret » et dont les services pourraient être retenus par les employés du SCRS; élabore et mette en œuvre une politique prescrivant à ses enquêteurs de faire état de tout conflit d'intérêts si quelque un leur demande leur opinion concernant les services d'un avocat à qui recourir;
- élabore et mette en œuvre une politique prescrivant à ses employés de fournir les renseignements pertinents en temps utile;
- modifie sa politique relative à la destruction des documents d'enquête sur une infraction à la sécurité ou d'enquête disciplinaire, dont les audiocassettes et les notes; rappelle à ses employés que la loi confère au CSARS le droit d'accès à toute information qui relève du SCRS – sauf les documents confidentiels du Cabinet – dont les audiocassettes, les notes manuscrites et les messages électroniques, et qu'il faut veiller à ne pas détruire des informations qui pourraient affecter la capacité du CSARS à exercer son droit d'accès à ces informations;
- mette d'avantage l'accent sur les obligations des employés relatives à la protection des renseignements classifiés, dans son cours d'orientation et dans les autres exposés sur la sécurité.

Présumées actions du SCRS lors d'une entrevue de citoyen

Rapport n° 2006-02

Le CSARS a fait rapport d'une décision concernant une plainte présentée en vertu de l'article 41 de la *Loi sur le SCRS* à l'égard de présumées actions du SCRS lors d'une entrevue de citoyen.

Le CSARS a conclu que le SCRS avait omis d'envoyer un avis en bonne et due forme au plaignant avant de tenir l'entrevue de citoyen. Il a constaté que, même si le rapport du SCRS à Citoyenneté et Immigration Canada contenait certaines erreurs, il rendait bien le contenu de l'entrevue de citoyen du plaignant.

Recommandation

- Le CSARS a recommandé que le SCRS instaure une procédure pour vérifier si les personnes à qui il est sur le point de faire subir une entrevue de citoyen ou d'immigration ont eu un préavis écrit suffisant de Citoyenneté et Immigration Canada, les informant que le SCRS compte les interviewer.

Révocation d'une habilitation de sécurité

Rapport n° 2006-03

Le CSARS a fait rapport d'une décision à l'égard d'une plainte présentée en vertu de l'article 42 de la *Loi sur le SCRS* au sujet de la révocation de l'habilitation de sécurité d'un employé du SCRS, qui a finalement mené au licenciement de l'intéressé.

Le plaignant avait une cote de sécurité « Très secret ». Selon la Politique du gouvernement sur la sécurité, une telle cote ne peut être octroyée s'il existe des motifs raisonnables de douter de la loyauté du demandeur envers le Canada ou de sa fiabilité personnelle à cet égard.

Depuis, le SCRS a informé le CSARS que CIC faisait désormais part aux personnes convoquées à une entrevue relative à l'immigration du fait que leur entrevue doit être menée par le Service, ou non.

D. Décisions du CSARS à l'égard des plaintes 2006-2007

Voici les résumés des cinq rapports que le CSARS a remis au cours de la période à l'étude en réponse aux plaintes reçues.

Discrimination présumée dans un processus d'immigration

Rapport n° 2006-01

Le CSARS a fait rapport d'une décision à l'égard d'une plainte dont l'avait saisi la Commission canadienne des droits de la personne en vertu de l'article 45 de la *Loi canadienne sur les droits de la personne*. Dans cette affaire, le plaignant alléguait avoir été l'objet de discrimination en contravention à cette loi après s'être vu refuser une « habilitation de sécurité⁸ ». Comme le plaignant avait besoin de cette habilitation dans le processus d'immigration, ce refus l'a empêché de devenir citoyen canadien.

Dans la plainte, il était normalement allégué : un retard du SCRS à traiter l'évaluation de sécurité du plaignant, qui a servi de fondement aux conseils fournis au ministre de la Citoyenneté et de l'Immigration en vertu de l'article 14 de la *Loi sur le SCRS*; des accusations portées par le SCRS contre le plaignant lors d'une entrevue subie par celui-ci; et un piètre traitement de la part du Service au cours d'un examen polygraphique.

Le CSARS a conclu à l'absence de preuves étayant les allégations relatives au retard du Service à traiter l'évaluation de sécurité ou à la conduite de l'entrevue de citoyenneté et de l'examen polygraphique. Le CSARS a conclu que le Service n'avait pas mené son enquête dans le but de traiter le plaignant de façon défavorable en raison de son origine nationale ou ethnique. Le SCRS avait plutôt enquêté sur des craintes qui étaient liées à la sécurité et avaient trait à la demande de citoyenneté canadienne du plaignant.

Recommandation

- Le CSARS a recommandé que la Commission canadienne des droits de la personne ne fasse pas enquête sur cette plainte.

⁸ La plainte originale contient le terme « habilitation de sécurité ». Il est à noter que le SCRS fournit des *evaluations* de sécurité, qui constituent le fondement des autorisations données par le ministre de la Citoyenneté et de l'Immigration. Le SCRS lui-même n'octroie pas d'habilitations dans ces cas-là. Pour plus d'information sur le processus de filtrage de sécurité, voir la section 2 du présent rapport.

Détermination de la compétence du CSARS à examiner une plainte...

...en vertu de l'article 41

Selon l'article 41 de la Loi sur le SCRS, le CSARS est tenu de faire enquête sur les plaintes que « toute personne » peut porter contre « des activités du Service ». Pour qu'il fasse enquête, deux conditions doivent être remplies :

1. le plaignant doit d'abord avoir présenté sa plainte par écrit au directeur du SCRS sans recevoir de réponse dans un délai raisonnable (environ 30 jours) ou, s'il en a reçu une, sans que cette réponse le satisfasse;

2. le Comité doit être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet ni entachée de mauvaise foi.
- Le CSARS ne peut enquêter sur une plainte qui peut être réglée autrement, par une procédure de griefs en vertu de la Loi sur le SCRS ou de la Loi sur les relations de travail dans la fonction publique.

...en vertu de l'article 42

Quant aux habilitations de sécurité, le CSARS est tenu, selon l'article 42 de la Loi sur le SCRS, d'enquêter sur les plaintes présentées par :

1. les personnes qui ne sont pas embauchées par le gouvernement fédéral à cause du refus d'une habilitation de sécurité;

2. les fonctionnaires fédéraux qui sont renvoyés, rétrogradés ou mutés ou qui se voient refuser une promotion ou une mutation pour la même raison;
3. les personnes qui se voient refuser un contrat de fourniture de biens ou de services au gouvernement, ou de services pour le même motif.

Les plaintes de ce type doivent être présentées dans les 30 jours du refus d'une habilitation de sécurité. Le CSARS peut prolonger ce délai si on lui fait part de raisons valables.

Tableau 1
Règlement des plaintes

	2004-2005	2005-2006	2006-2007
Reportées de l'exercice précédent	16	18	24
Nouvelles	30	45	37
Total	46	63	61
Réglées	28	39	41
Reportées à l'exercice suivant	18	24	20
Rapports	3	4	5

Les types de plaintes sur lesquelles le CSARS enquête sont décrits dans la *Loi sur le SCRS* et prennent diverses formes.

En vertu de l'article 41 de la *Loi sur le SCRS*, le CSARS peut enquêter sur n'importe quelles « activités du Service ». Selon l'article 42, il peut instruire les plaintes concernant le refus d'habilitations de sécurité à des fonctionnaires et à des fournisseurs de l'État. L'article 42 ne l'autorise pas à reconnaître sa compétence à instruire les plaintes concernant les contrôles d'antécédents ou les vérifications de fiabilité, à caractère moins intrusif, qui sont menés simplement pour déterminer la loyauté ou l'aptitude d'un fonctionnaire fédéral éventuel. Pour l'étude de ces plaintes, on suit la procédure de grief prévue par l'organisme intéressé.

Selon l'article 42 de la *Loi sur le SCRS*, les personnes qui se voient refuser une habilitation de sécurité doivent en être avisées par l'administrateur général de leur organisme. Elles ont le droit de porter plainte au CSARS qui, s'il y a lieu, fait enquête et présente ses constatations et recommandations au Ministre, au directeur du SCRS, à l'administrateur général concerné et au plaignant.

Si la Commission canadienne des droits de la personne reçoit d'un ministre un avis écrit concernant une plainte qui a trait à la sécurité du Canada, elle peut en saisir le CSARS. Sur réception d'un tel renvoi, le Comité fait enquête et lui présente ses constatations, ainsi qu'au directeur du SCRS, au ministre de la Sécurité publique, au ministre compétent et au plaignant. Il a aussi le pouvoir d'enquêter sur les affaires qui lui sont renvoyées en vertu de la *Loi sur la citoyenneté*.

Une fois terminée son enquête sur une plainte présentée en vertu de l'article 41, le CSARS présente un rapport de ses constatations et recommandations au directeur du SCRS, au ministre de la Sécurité publique et au plaignant⁷. Les résumés de ces rapports, expurgés de manière à protéger la sécurité nationale et la vie privée des intéressés, figurent également dans le rapport annuel du CSARS au Parlement.

Le tableau 1 montre l'état de toutes les plaintes qui ont été présentées au CSARS au cours des trois derniers exercices, y compris celles qui lui ont été adressées à tort, qui ont été déclarées hors de sa compétence ou qui ont fait l'objet d'une enquête et d'un règlement sans audience (examen administratif).

Le plaignant reçoit une version déclassifiée du rapport.

C. Enquêtes sur les plaintes

PROCÉDURE D'ENQUÊTE DU CSARS SUR LES PLAINTES

Outre sa fonction de surveillance, le Comité a charge d'enquêter sur les plaintes du public au sujet du SCRS. La première étape de presque tous les dossiers de plainte est une demande de renseignements qui peut être présentée au CSARS par écrit, en personne ou par téléphone. Le personnel du Comité y répond sur-le-champ, indiquant généralement au plaignant éventuel les exigences de la *Loi sur le SCRS* pour que son affaire soit considérée à titre de plainte officielle.

Lorsqu'il reçoit une plainte par écrit, le CSARS en fait un examen initial. Si elle ne répond pas à certaines exigences de la loi, le CSARS ne reconnaît pas sa compétence et n'enquête pas. S'il la reconnaît, il étudie la plainte lors d'une audience quasi judiciaire que préside un ou plusieurs de ses membres, secondés par le personnel.

Dans ses enquêtes sur les plaintes, le CSARS a tous les pouvoirs d'une cour supérieure et il a accès à toute information que le SCRS a en main, sauf les documents confidentiels du Cabinet.

Un plaignant a le droit d'être représenté par un avocat et de formuler des observations à l'audience. Une audience préliminaire peut être tenue pour arrêter une procédure, de concert avec le plaignant ou son avocat, ou avec les deux. L'avocat principal du Comité fournit des avis juridiques concernant la procédure et les questions de fond et il contre-interroge aussi les témoins du Service si ceux-ci doivent être entendus en l'absence du plaignant, pour des raisons liées à la sécurité nationale.

Types de plaintes

- Le CSARS peut faire enquête sur quatre types d'affaires :
- les plaintes de particuliers « contre des activités du Service » (article 41);
 - celles concernant le refus d'habilitations de sécurité à des fonctionnaires et à des fournisseurs de l'État (article 42);
 - les allégations dont la Commission canadienne des droits de la personne saisit le CSARS;
 - les rapports du Ministre à l'égard de la *Loi sur la citoyenneté*.

Jabarah est un terroriste mais aussi un citoyen canadien et, si ignobles que soient ses actes, la *Charte* lui confère certains droits fondamentaux. Le CSARS a pour mission de protéger les droits des Canadiens en veillant à ce que le SCRS respecte la loi. En conséquence, celui-ci doit respecter la *Charte* dans la conduite de ses enquêtes, selon le mandat que lui confère la *Loi sur le SCRS*, quelles que soient les circonstances imprévues qui peuvent survenir.

Conclusion

- mandat selon l'article 12 de la *Loi sur le SCRS*.
- Charte*, et en toute occasion où il n'est pas clair que l'activité du Service entre dans son entraîner sa détention, afin d'assurer le respect des droits de l'intéressé en vertu de la opération amenant à interroger un individu dans des circonstances qui peuvent
- Que le SCRS demande et obtienne du ministre de la Justice un avis écrit pour toute *personnel, sur l'accès à l'information et sur la Bibliothèque et les Archives du Canada*.
 - informations opérationnelles qui relèvent de lui, dont les courriels, soient conformes aux lois fédérales applicables, y compris les *Lois sur le SCRS, sur la protection des renseignements*
 - Que le SCRS veille à ce que le stockage, la conservation et la recherche de toutes les officielles et non officielles auprès des ministères des Affaires étrangères et de la Justice. mesure du possible, y compris mais non de façon limitative de ses consultations
 - Que le SCRS conserve des documents de ses consultations interministérielles, dans la conservé selon les lois fédérales applicables.
 - par opposition à « document éphémère », et du fait qu'il doit donc être classé et
 - Que le SCRS informe clairement ses employés de ce qu'est un « renseignement consigné », à moins d'une décision délibérée de les supprimer.
 - Que le SCRS modifie ses politiques de façon que les courriels soient conservés d'office,

Jabarah ne pouvait être poursuivi pour aucun crime au Canada, car ses activités terroristes étaient antérieures à l'adoption de la *Loi antiterroriste* au pays. Ni le SCRS ni la police n'avaient le droit de le détenu. Compte tenu de ces circonstances, entre autres, le Comité a conclu que le SCRS avait « détenu arbitrairement » Jabarah en violation de l'article 9 de la *Charte*. En le détenu, on a violé son droit au silence, protégé par l'article 7 et l'alinéa 11c), tout comme celui à l'assistance d'un avocat en vertu de l'article 10. De plus, on a foulé aux pieds son droit de demeurer au Canada, protégé par l'article 6 de la *Charte* (liberté de circulation).

Un autre organisme canadien a informé le SCRS que Jabarah ne pouvait être inculpé au criminel puisque les actes qu'il avait posés n'avaient pas eu lieu au Canada et n'y étaient pas tenus pour des crimes à l'époque. Cependant, le SCRS savait que Jabarah pouvait être poursuivi aux États-Unis. Au fil de son étude, le CSARS a appris que des actions (qui restent classifiées) du SCRS avaient aidé de façon appréciable les représentants des organismes américains d'application de la loi. Pour cette raison, il estime que le SCRS ne pouvait être indépendant par rapport aux consultations qu'il a eues auprès de Jabarah. Ces actions ont en outre amené le CSARS à conclure que le SCRS avait dérogé à son mandat de renseignement de sécurité pour s'occuper d'exécution de la loi.

Enfin, le CSARS a constaté qu'il manquait certains documents pertinents à son étude. Il a relevé des mentions de réunions dont on n'avait pas les procès-verbaux et de consultations interministérielles dont il n'existait aucun document officiel ainsi que de courriels opérationnels supprimés. Ces lacunes des documents officiels lui ont inspiré des craintes. Ce qui l'a particulièrement inquiété, c'est que le SCRS ait pu mener une enquête d'une telle importance et aussi délicate – l'enquête avait eu une incidence directe sur la mise en accusation et la poursuite d'un Canadien par les autorités américaines – sans demander l'avis juridique officiel du ministre de la Justice.

Recommandations

Le CSARS a formulé six recommandations par suite de cette étude :

- Que le protocole d'entente conclu en 1987 entre le SCRS et le ministère des Affaires étrangères et du Commerce international soit mis à jour et désigne ce ministère à titre d'organisme principal dans les affaires de citoyens canadiens détenus à l'étranger. Le protocole devrait aussi refléter celui recommandé par le juge O'Connor, à savoir « des consultations franches et à point nommé entre les organismes canadiens » qui peuvent avoir un rôle à jouer à l'égard des Canadiens détenus à l'étranger, « une démarche cohérente et unifiée » menée par le MABCI et « la reddition de comptes à l'égard des mesures adoptées » en pareil cas.

Constatations

Cette étude met en lumière un débat beaucoup plus vaste qui a cours dans la plupart des démocraties occidentales. Dans une allocution prononcée en novembre 2004, le juge Ian Binnie, de la Cour suprême du Canada, a qualifié de « combat de titans » les intérêts antagonistes de la sécurité nationale et des droits de la personne.

Ayant étudié cette affaire, le CSARS reconnaît que le contexte des événements était tel, peu après le 11 septembre, que la protection du Canada et la coopération avec ses alliés proches étaient des priorités dans toute la collectivité du renseignement de sécurité. Le SCRS croyait, a-t-on appris au CSARS, que Jabarah avait consenti de façon libre et volontaire à coopérer avec lui et à abandonner sa liberté à un pays étranger.

Néanmoins, le Comité a abordé cette étude en sachant que l'article 32 de la *Charte* s'applique aux actions du SCRS. Les instructions ministérielles renforcent en outre l'obligation du SCRS de respecter la *Charte*. En raison d'événements survenus pendant le séjour de Jabarah au Canada et étant donné que le SCRS a aidé à organiser son transport aux États-Unis à bord d'un avion du gouvernement canadien, le CSARS s'est employé à vérifier si le SCRS avait exercé une diligence raisonnable dans le but d'assurer la conformité de ses actions aux règles de droit canadiennes.

Dans son étude, le CSARS a soulevé des questions quant à la thèse du SCRS voulant que les décisions de Jabarah aient été prises de façon libre et volontaire. Il partage l'avis du juge LaForest, à savoir que plusieurs circonstances entourant cette affaire inciteraient un tribunal à scruter avec soin les actions des représentants du SCRS afin de déterminer si les décisions de Jabarah étaient tout à fait volontaires. Ces décisions, prises sans le bénéfice d'un avis juridique indépendant, ont amené Jabarah à s'incriminer lui-même et à se rendre aux autorités américaines. Le CSARS croit qu'un tribunal aurait aussi tenu compte d'autres facteurs : l'âge de l'intéressé; son état émotif; la possibilité que sa crainte des solutions de rechange ait joué dans son retour d'Oman au Canada; le temps qu'il a passé en compagnie des représentants du SCRS lorsqu'il était au Canada; et les circonstances entourant sa décision de se faire extraditer dans un pays étranger.

Un enquêteur du SCRS a dit au CSARS qu'on n'avait pas « fait lecture de ses droits » à Jabarah parce que le SCRS n'est pas un service de police. Cette réponse, que le Service a par la suite confirmée par écrit, montre une mauvaise compréhension de l'application de la *Charte* à l'exercice des fonctions officielles des représentants du gouvernement.

Néanmoins, en dépit de ses aveux, Jabarah ne pouvait être inculpé en vertu du *Code criminel*, car toutes ses activités terroristes étaient antérieures à l'adoption de la *Loi antiterroriste* canadienne. Le SCRS l'a consulté, ce qui l'a amené à signer un accord facilitant son entrée aux États-Unis. En mai 2002, Jabarah y a été transporté avec l'assistance du SCRS et il a par la suite plaidé coupable à diverses infractions liées au terrorisme. Au moment où le SCRS mettrait la dernière main à son étude, Jabarah n'avait pas encore été condamné et il demeure incarcéré.

Le CSARS a décidé de citer le nom de cet individu dans son rapport annuel étant donné qu'une information très abondante au sujet de cette affaire est déjà du domaine public. Le 14 août 2007, le commissaire à la protection de la vie privée a été informé de sa décision. Cela a été fait en vertu de l'article 8(2)m) de la *Loi sur la protection des renseignements personnels*, qui autorise la communication de renseignements personnels lorsque « des raisons d'intérêt public justifiaient nettement une éventuelle violation de la vie privée ».

Méthode

Le CSARS a examiné cette enquête par rapport à la politique opérationnelle et aux procédures du SCRS, aux instructions ministérielles et aux règles de droit canadiennes applicables, dont la *Loi sur le SCRS* et la *Charte canadienne des droits et libertés*. Il a aussi été attentif à deux faits, soit que Jabarah est un citoyen canadien et que les représentants du Canada doivent agir dans le respect de la loi.

Le CSARS a étudié les documents classifiés, en versions électronique et imprimée, concernant : le rôle du SCRS durant le séjour de Jabarah à Oman et son retour accompagné de la-bas au Canada; après son retour au pays; et son transfertement sous garde américaine. Le Comité a aussi examiné des documents non classifiés, de sources ouvertes (un livre, des lettres, des articles de presse, etc.). De plus, il a reçu un exposé général du SCRS et un exposé approfondi des enquêteurs affectés à cette affaire. Le CSARS a aussi obtenu un avis juridique de l'ancien juge de la Cour suprême du Canada, M. Gérard LaForest, C.C., c.r., spécialiste réputé de la *Charte*.

En raison de la nature et de la gravité des questions soulevées dans son étude, le Comité a décidé de présenter ses constatations et recommandations directement au ministre de la Sécurité publique en vertu de l'article 54 de la *Loi sur le SCRS*.

B. Rapport en vertu de l'article 54

L'article 54 de la *Loi sur le SCRS* habilite le CSARS à présenter au ministre de la Sécurité publique un rapport spécial sur toute question qui relève de sa compétence. Le CSARS a conclu que les événements auxquels avait été mêlé Mohammed Mansour Jabarah, de même que les préoccupations soulevées par l'Association canadienne des libertés civiles, étaient suffisamment importants pour justifier un tel rapport.

En avril 2005, la ministre d'alors à la Sécurité publique a écrit à l'Association canadienne des libertés civiles pour l'assurer que les actions du SCRS avaient été « irréprochables et conformes à son mandat » dans cette enquête. Le Comité ne sait pas sur quel avis la lettre de la Ministre est fondée, mais d'après son analyse, l'article 12 de la *Loi sur le SCRS* n'aurait pas autorisé tous les volets de l'enquête. Cela sert à rappeler l'importance que les ministres bénéficient d'un avis exact et complet sur des questions aussi délicates.

Étude de l'affaire Mohammed Mansour Jabarah

Étude n° 2005-05

Contexte

Le citoyen canadien Mohammed Mansour Jabarah est, de l'aveu de tous, membre d'Al-Qaïda et chef de la cellule terroriste qui avait ourdi des attentats à la bombe contre les ambassades américaines et israéliennes à Singapour et à Manille. Si ce plan avait réussi, cela aurait pu être catastrophique. Cependant, le plan ayant été contrarié, Jabarah s'est enfui et a été appréhendé à Oman en mars 2002. Au pied levé, des représentants du SCRS se sont rendus à Oman et se sont vus inopinément dans l'obligation de prendre des dispositions pour le retour de Jabarah au Canada. Le SCRS a payé son billet.

Cette enquête a été inhabituelle, sinon unique, sur plusieurs plans. Dans la foulée du 11 septembre, le Canada se donnait beaucoup de peine pour en apprendre le plus possible sur la menace que représentait Al-Qaïda et pour se montrer un proche allié fiable des États-Unis dans la lutte au terrorisme.

Dans une allocution prononcée en octobre 2006 à la conférence de l'Association canadienne pour les études de renseignement et de sécurité, le directeur du SCRS, Jim Judd, a reconnu la chose en ces termes : « L'espionnage étranger prend de l'ampleur et une forme de plus en plus sophistiquée grâce aux nouvelles technologies ».

L'un des moyens mis en œuvre par le Service pour enrayer cette menace est l'Unité des enquêtes de contre-espionnage. Elle a été mise sur pied en 2002 afin de cloisonner, en matière de contre-espionnage, les délicates enquêtes susceptibles d'amener à poursuivre les personnes qui fournissent sciemment des renseignements ou des biens de nature délicate, d'une manière préjudiciable aux intérêts canadiens, à des services de renseignement ou à des gouvernements étrangers qui sont hostiles.

Méthode

Dans son étude, le CSARS a scruté les activités exercées par l'Unité des enquêtes de contre-espionnage pour en évaluer la conformité avec la *Loi sur le SCRS* ainsi qu'avec les instructions ministérielles et les politiques opérationnelles. Il a aussi examiné la manière dont le Service enquête et dont il soutient la poursuite des infractions en matière de contre-espionnage en partageant des informations avec les organismes d'exécution de la loi.

Le CSARS a choisi deux enquêtes pour en faire une étude approfondie. Dans chaque cas, il a examiné les décisions d'enquêter, les activités d'enquête, les rapports opérationnels ainsi que la coopération et les échanges d'information avec les partenaires canadiens et étrangers. En raison du caractère délicat de ces affaires, le CSARS ne peut fournir plus de détails dans ce rapport.

Constatations

Le CSARS a constaté que le Service s'était conformé à la *Loi sur le SCRS*, aux instructions ministérielles et aux politiques opérationnelles dans ses enquêtes de contre-espionnage.

En ce qui touche la première enquête, le CSARS a conclu que la coopération étroite entre le SCRS et ses homologues canadiens et étrangers avait permis de régler un « grave problème de sécurité » de façon utile et efficace.

Quant à la seconde, le CSARS a conclu que la communication d'informations par le SCRS avait permis à la GRC de prendre des mesures contre quelqu'un qui se livrait à des activités illicites.

Cette étude n'a donné lieu à aucune recommandation.

Recommandations

Le CSARS a formulé deux recommandations par suite de cette étude :

- Il a noté un manque de gradation, dans les notes d'information, entre les divers degrés du risque posé par les sujets de filtrage de sécurité. Ainsi, les évaluations du Service, à l'égard des liens d'un sujet avec des individus que l'on savait ou croyait menacer la sécurité nationale, étaient fondées sur des renseignements que le CSARS considérait moins déterminants dans certains cas que dans d'autres. Dans un autre exemple, certains sujets de filtrage de sécurité, mais pas tous, ont eu la possibilité de discuter de questions de sécurité dans une entrevue avec la Direction du filtrage de sécurité. Le CSARS a trouvé inquiétant que les notes d'information ne comportent pas de gradation correspondant aux divers degrés du risque posé par les postulants au filtrage, et qu'elles ne soient ni uniformes ni cohérentes, contrairement à la politique. En conséquence, il a recommandé que le Service élabore une politique pour régler cette question.
- Le CSARS a noté qu'à mi-parcours de la période à l'étude, le Service avait cessé de conserver par écrit les formulaires de consentement aux évaluations de sécurité effectuées pour un organisme étranger, de sorte qu'il était impossible de savoir si le consentement avait bien été demandé et obtenu. Le CSARS a recommandé que le SCRS obtienne des formulaires de consentement écrit aux évaluations de sécurité dans les cas où il ne peut y avoir accès après le fait (soit dans le cas des organismes étrangers).

Étude n° 2006-08

Note :

L'étude n° 2006-08 n'était pas terminée au moment de mettre sous presse. Un résumé en sera présenté dans le Rapport annuel du CSARS 2007-2008.

Examen de l'Unité des enquêtes de contre-espionnage du SCRS

Étude n° 2006-09

Contexte

Depuis le 11 septembre, les services de renseignement occidentaux axent de plus en plus leur attention et leurs ressources sur les enquêtes antiterroristes, mais il reste d'autres menaces à la sécurité dont il faut s'occuper. En 2006, le SCRS et d'autres autorités fédérales ont pris part à l'arrestation et à l'expulsion d'un espion russe qui vivait au Canada depuis plusieurs années sous une fausse identité. Cette affaire rappelle que le Canada demeure une cible de l'espionnage étranger.

- accède aux demandes d'organismes étrangers (au moyen d'ententes avec les pays concernés) au sujet des Canadiens qui postulent, dans un pays étranger, un emploi requérant l'accès à des documents classifiés;
- fournit des évaluations de sécurité pour les programmes non liés à l'obtention d'une core de sécurité et concernant notamment les centrales nucléaires, la cité parlementaire, les gouvernements provinciaux et les sites intéressant la sécurité nationale (p. ex., les aéroports et ports), et pour d'autres programmes.

Il est à noter que certains programmes sont régis par la Politique du gouvernement sur la sécurité, tandis que d'autres, tels le Programme d'autorisation d'accès aux zones réglementées d'aéroports et le programme Expéditions rapides et sécuritaires, sont exécutés en vertu d'autorisations et de seuils différents.

Cette étude a porté sur les évaluations destinées aux programmes qui ne sont pas liés à l'obtention d'une core de sécurité.

Méthode

Le CSARS a évalué la conformité du Service à la *Loi sur le SCRS*, aux instructions ministérielles, aux politiques opérationnelles, à la Politique du gouvernement sur la sécurité et aux protocoles d'entente pertinents entre le Service et ses clients. Le CSARS a effectué une étude approfondie d'un échantillon de cas échelonnés sur six mois et une analyse détaillée de toutes les notes d'information⁷ remises pendant la période considérée (aucun avis de refus n'a été donné pendant la période à l'étude), qui s'étend du 1^{er} avril 2004 au 31 mars 2006.

Constatations

Le CSARS a constaté un manque considérable d'uniformité dans les notes d'information et des incohérences dans les enregistrements et les transcriptions d'entrevues destinés à servir dans ces notes⁸. Il a noté avec satisfaction que le Service avait effectué des contrôles de sécurité uniquement pour les organismes étrangers avec lesquels il avait conclu une entente approuvée et que, suivant la politique, il n'avait fait aucune recommandation à des entités étrangères. Enfin, le Service s'était conformé aux instructions ministérielles en conservant l'information sur le filtrage de sécurité séparément de ses autres fonds de renseignements, en raison du caractère délicat qu'elle revêt pour les personnes soumises à une évaluation.

⁷ Dans les cas de filtrage pour le gouvernement, le SCRS remet des notes d'information s'il découvre des informations qui pourraient susciter des craintes. Il les remet à l'organisme demandeur qui décide alors s'il y a lieu, ou non, d'octroyer à un candidat une habilitation de sécurité ou d'accès à des sites.

⁸ Depuis, le Service a modifié sa politique relative aux entrevues.

Le CSARS a déjà noté que l'arrêt *R. c. Stinchcombe*, rendu en 1991 par la Cour suprême et obligeant la Couronne à communiquer toute information pertinente à l'avocat de la défense, « a remis en question » le mécanisme d'échange d'informations, en particulier l'obligation qui incombe à la GRC d'obtenir l'autorisation expresse du SCRS avant d'utiliser des renseignements de celui-ci dans une poursuite judiciaire. En 2007, le SCRS et la GRC ont créé un groupe de travail pour examiner et améliorer le processus d'utilisation des renseignements de sécurité dans les poursuites criminelles pour infractions en matière de sécurité nationale.

Cette étude n'a donné lieu à aucune recommandation.

Étude du filtrage de sécurité à l'extérieur de l'administration fédérale

Étude n° 2006-07

L'article 13 de la *Loi sur le SCRS* habilite le Service à fournir des évaluations de sécurité aux gouvernements fédéral et provinciaux ainsi qu'aux services de police et aux entités étrangères. L'objectif du programme Filtrage de sécurité est double : empêcher un non-Canadien, qui suscite des inquiétudes ou présente des risques quant à la sécurité, d'entrer au Canada ou d'y obtenir la résidence permanente; et, empêcher toute personne qui suscite des inquiétudes quant à la sécurité d'être autorisée à avoir accès à des biens, à des endroits ou à des informations du gouvernement.

Les évaluations de sécurité du SCRS entrent dans deux grandes catégories de programmes :

1. Immigration, par lequel le Service fournit des évaluations de sécurité à Citoyenneté et Immigration Canada et à l'Agence des services frontaliers du Canada pour appuyer le traitement des demandes de candidats au statut de réfugié ainsi qu'à l'immigration et à la citoyenneté;
2. Filtrage de sécurité pour le gouvernement, par lequel le Service :
 - fournit des évaluations de sécurité à tous les ministères et organismes fédéraux, sauf à la GRC;

Rapport n° 101, Coopération du SCRS avec la Gendarmerie royale du Canada, partie 1, document dont il est fait état dans la section 1 du Rapport annuel du CSARS 1997-1998.

Pour plus d'information sur les activités du SCRS en matière de filtrage de sécurité, prière de vous reporter à la section 2 du présent rapport annuel.

À cette fin, le CSARS a étudié tous les échanges d'information avec la GRC, tous les dossiers ayant trait aux relations du SCRS avec elle, à l'administration centrale et dans deux bureaux régionaux, et tous les documents concernant les relations du SCRS avec deux équipes intégrées de la sécurité nationale pendant l'année civile 2005². Le CSARS s'est aussi penché sur le ciblage de deux individus, par le SCRS, entre le 1^{er} janvier et le 31 juillet 2005.

Au sujet de l'organisme étranger, le CSARS a examiné tous les échanges d'information entre 2001 et 2005, les évaluations de cet organisme effectuées par le SCRS en 2001 et 2006 ainsi que tous les dossiers ayant trait à leurs relations mutuelles pendant l'année civile 2005.

Constatations

Les échanges d'information du SCRS avec l'organisme étranger respectaient la portée de l'entente conclue avec lui et étaient conformes à la *Loi sur le SCRS*, aux instructions ministérielles et aux politiques opérationnelles pertinentes. Les mauvaises communications internes ont préoccupé le Comité, car certains agents du SCRS ne connaissaient pas l'état des relations de celui-ci avec l'organisme étranger pendant la période 2002-2004. Cela a fait que la mission confiée à l'ALS était inexacte. Il n'y a cependant eu aucun échange d'information réprouvable.

Les échanges d'information du SCRS avec la GRC étaient autorisés en vertu de la *Loi sur le SCRS* et conformes aux instructions ministérielles et aux politiques opérationnelles pertinentes. En ce qui touche les relations du SCRS et de la GRC de façon plus générale, le CSARS a noté la bonne volonté qui régnait entre les deux organismes et dont témoignaient le nouveau protocole d'entente signé le 12 septembre 2006 et d'autres initiatives. Ce nouveau protocole remplace l'original, signé en 1990, qui était devenu périmé. Cependant, il subsiste certaines difficultés. Le Comité a relevé deux cas qui ont semblé susciter des frictions de grande portée entre le SCRS et la GRC en 2005. Le premier est une tentative de poursuite de la GRC, qui a fait appel à des renseignements du SCRS. Le second concerne les activités d'une source humaine de celui-ci, qui a compliqué une enquête de la GRC aux fins d'une poursuite au criminel. Le CSARS note cependant des faits nouveaux positifs, sur le plan des relations du SCRS et de la GRC dans cette région, depuis 2005.

² D'autres renseignements sur le programme des Équipes intégrées de la sécurité nationale sont fournis à la section 2 du Rapport annuel du CSARS 2002-2003.

Constatations

Dans l'ensemble, le CSARS a conclu que le Service s'était conformé à la *Loi sur le SCRS* ainsi qu'aux instructions ministérielles et aux politiques opérationnelles dans son enquête sur les cibles. L'information qu'il avait recueillie ne montrait pas que les membres du groupe avaient pris part à des activités terroristes pendant leur séjour au Canada et il a donc conclu qu'ils ne constituaient pas une cellule terroriste opérationnelle, active au pays. Le CSARS s'est rallié à l'évaluation du SCRS selon laquelle celui-ci avait des motifs raisonnables de soupçonner que les activités des principales cibles représentaient une menace possible à la sécurité du Canada.

Cette étude n'a donné lieu à aucune recommandation.

Étude de la collaboration et des échanges de renseignements du SCRS à la suite du 11 septembre

Étude n° 2006-06

Contexte

Cette étude a été déclenchée, entre autres, en raison des changements survenus dans les relations du SCRS avec ses partenaires étrangers et canadiens à la suite du 11 septembre. Le SCRS échange davantage d'information que par le passé avec ses partenaires étrangers dont le nombre a en outre augmenté. Au Canada, le rôle de la GRC dans les enquêtes sur les menaces à la sécurité s'est élargi à la suite de l'adoption de la *Loi antiterroriste*, qui a criminalisé les actions mettant en cause la sécurité du pays. Aussi le SCRS est-il soumis à des pressions croissantes l'incitant à appuyer les poursuites de la GRC.

Méthode

Cette étude a porté sur les relations du SCRS avec l'un de ses partenaires étrangers et avec la GRC. L'objectif était d'évaluer la conformité du Service avec la *Loi sur le SCRS* ainsi qu'avec les instructions ministérielles, les protocoles d'entente et les politiques opérationnelles et, aussi, d'examiner le rendement du SCRS dans le contexte de ses relations avec la GRC.

Étude d'une enquête antiterroriste

Étude n° 2006-05

Contexte

Ce groupe étranger, notoire pour son appui à Al-Qaïda, a été parmi les premiers à figurer sur la liste canadienne d'entités terroristes. Cette étude du CSARS était sa première sur une enquête du Service au sujet d'une présumée activité liée à la menace, que ce groupe aurait exercée au Canada. Elle lui a fourni l'occasion de se pencher sur une certaine méthode d'enquête employée à l'occasion par le SCRS.

Méthode

Le CSARS a examiné l'enquête menée par le Service du 1^{er} janvier 2003 au 31 décembre 2005. Son objectif était de percer cette enquête et ses difficultés ainsi que d'évaluer la conformité du Service avec la *Loi sur le SCRS*, les instructions ministérielles et les politiques opérationnelles.

En particulier, le CSARS a examiné :

- l'enquête menée sur les membres présumés de ce groupe et les autorisations d'enquêtes;
- la mise en oeuvre des pouvoirs conférés par la Cour fédérale au moyen de mandats;
- leur exercice contre les principales cibles;
- la gestion des sources humaines, dont celles qui étaient en voie de formation;
- les conseils au gouvernement et les échanges d'information avec des organismes canadiens;
- les échanges d'information et la coopération avec des services de renseignement étrangers.

De plus, le CSARS a eu droit à deux exposés : un tour d'horizon de l'enquête du Service et une rencontre avec l'enquêteur principal du SCRS afin de discuter de l'interaction du Service avec les principales cibles.

Une entente conclue en 1987 par trois ministres définit les rôles et responsabilités des diverses parties à la collecte en vertu de l'article 16. L'une de ces parties est le Centre de la sécurité des télécommunications (CST), qui fournit l'assistance technique en matière de collecte de renseignements étrangers.

Les renseignements visés à l'article 16 et fournis par le CST au Service sont couramment assujettis au principe de la « divulgation minimale » afin de respecter les diverses instructions touchant l'interdiction d'enquêter sur des entreprises et des ressortissants canadiens. Ainsi, le nom d'une personne ou d'une entité canadienne, obtenu indirectement, serait signalé au Service par une expression comme « un ressortissant canadien » ou « une société canadienne ». Dans des circonstances précises, définies dans la politique du Service, si celui-ci peut démontrer que l'information a trait à des activités susceptibles de menacer la sécurité du Canada, selon la définition de l'article 2 de la *Loi sur le SCRS*, il peut demander l'identité des intéressés au CST.

Méthode

Le CSARS a examiné la collecte de renseignements recueillis par le SCRS sur un pays étranger (pays A) en vertu de l'article 16, évaluant cette activité par rapport à la *Loi sur le SCRS*, aux instructions ministérielles et notamment à cette entente conclue par trois ministres en 1987. Il s'est normalement penché sur ce qui suit :

- tous les rapports fournis au ministère des Affaires étrangères et du Commerce international (MAECI) en 2005 en vertu de l'article 16, et les réactions de ce ministère;
- les demandes de mandats et l'exercice des pouvoirs obtenus par ceux-ci en vertu de l'article 16 ainsi que le traitement des documents connexes;
- la gestion des sources humaines qui avaient fourni à la fois des renseignements étrangers et d'autres liés à la menace;
- l'autorisation d'une enquête correspondante sur des activités liées à la menace et tous les échanges d'information avec le MAECI fondés sur cette menace.

Le personnel du CSARS a aussi assisté à un exposé du SCRS et tenu des discussions officielles avec des employés de celui-ci.

Constatations

La collecte de renseignements étrangers par le SCRS sur le pays A respectait les exigences de la *Loi sur le SCRS*, ne ciblant aucune personne ni organisation canadienne. Les demandes de pouvoirs conférés par la voie de mandats et l'exercice de ces pouvoirs en vertu de l'article 16 ainsi que la gestion des sources humaines, qui ont fait l'objet de l'étude, étaient en outre appropriées et conformes aux exigences de la loi et des politiques.

Les échanges d'information du Service avec ses partenaires canadiens et étrangers étaient appropriés, sauf que des relations difficiles avec un organisme étranger ont nui à ses enquêtes de la période considérée. Le CSARS a aussi relevé un cas de mauvaise coordination entre la GRC et le SCRS qui en a perdu la trace d'un individu pendant plusieurs mois. Les deux organismes avaient échangé de l'information de façon irrégulière au sujet de l'intéressé. Par suite de la décision de la GRC de restreindre son enquête, le SCRS ne savait plus exactement où se trouvait l'individu. Il n'a pu le retrouver au cours des cinq mois suivants jusqu'à ce qu'il apprenne qu'il n'était plus au pays, ce sur quoi il a mis fin à son enquête.

Enfin, le CSARS a examiné le cas d'un citoyen canadien qu'un pays étranger avait détenu en raison de sa participation présumée à une activité terroriste. Selon les allégations des médias, l'intéressé avait subi de mauvais traitements pendant sa détention. Le CSARS a conclu que le Service avait mené une enquête efficace et appropriée sur les allégations de terrorisme et sur les présumés mauvais traitements subis pendant la détention. Il a aussi conclu que le SCRS avait confirmé sa responsabilité au ministère des Affaires étrangères et du Commerce international, qui était l'organisme principal dans ce dossier.

Cette étude n'a donné lieu à aucune recommandation.

Étude d'une activité visée à l'article 16

Étude n° 2006-04

Contexte

En vertu des dispositions de l'article 16 de la *Loi sur le SCRS*, le ministre de la Défense nationale ou celui des Affaires étrangères peut demander l'assistance du Service par écrit pour la collecte de renseignements étrangers au Canada. Renseignements étrangers se définit ainsi : informations ou renseignements sur les moyens, les intentions ou les activités d'un individu, d'un État, d'une organisation ou d'un groupe terroriste étrangers, en ce qui touche les affaires internationales, la défense ou la sécurité.

Si le ministre de la Sécurité publique approuve la demande, elle est transmise au directeur du Service, accompagnée de son consentement écrit et d'instructions. Le SCRS ne peut stocker les renseignements étrangers recueillis, dans sa base de données visées à l'article 12 de la *Loi sur le SCRS*, que s'ils facilitent ses enquêtes relevant de cet article.

La *Loi* interdit expressément de diriger toute collecte de renseignements visés à l'article 16 contre des citoyens canadiens, des immigrants admis ou des sociétés canadiennes. Si le SCRS choisit de ne pas stocker ces renseignements pour une enquête menée au terme de l'article 12, la compétence du CSARS prend fin lorsque les renseignements ont été transmis au ministre qui en avait fait la demande.

Méthode

C'était la première fois que le CSARS se penchait sur cette enquête particulière. Il a analysé les documents ayant trait aux enquêtes sur les personnes soupçonnées de se livrer à des activités menaçantes, la direction de sources humaines contre les cibles autorisées et tous les échanges d'information avec des organismes canadiens et étrangers.

Constatations

L'identification des cibles par le Service et ses enquêtes sur leur compte ont été trouvées en tous points conformes à la *Loi sur le SCRS* ainsi qu'aux instructions ministérielles et aux politiques opérationnelles applicables. Dans chaque enquête, le SCRS avait des motifs raisonnables de soupçonner l'existence d'une menace et les autorisations d'enquête allaient de pair avec la gravité des menaces. Ses enquêteurs ont recueilli uniquement des informations strictement nécessaires aux enquêtes.

Le CSARS a noté que l'enquête avait manqué de ressources tout au long de la période considérée et que la responsabilité administrative de ce dossier était passée à plusieurs reprises d'un module opérationnel à un autre, au SCRS. Cela a eu des conséquences néfastes sur la gestion de l'information et, dans une certaine mesure, sur celle des sources humaines. En général, le CSARS a toutefois constaté que le SCRS a respecté les politiques opérationnelles dans le traitement de ses sources humaines.

En vertu de l'article 2 de la *Loi sur le SCRS*, il est interdit d'enquêter sur les personnes qui prennent part à des activités illicites de défense d'une cause, de protestation ou de manifestation d'un désaccord, à moins que ces activités ne coïncident avec des menaces à la sécurité du Canada. Selon la politique opérationnelle, il est donc prescrit que les enquêtes mettant au jour de telles activités fassent l'objet d'une autorisation spéciale de la haute direction.

Le CSARS a relevé un cas où l'on n'a pas satisfait aux exigences de la politique opérationnelle. Le Service enquêtait sur plusieurs membres d'un centre communautaire canadien, croyant qu'ils se livraient à des activités menaçantes, étrangères aux activités illicites du centre en matière de défense d'une cause, de protestation ou de manifestation d'un désaccord. L'étude du CSARS a confirmé que l'enquête du Service ne visait pas ces activités. Néanmoins, la politique opérationnelle requiert une autorisation émanant de la haute direction en raison de la participation de ces personnes à de telles activités. Le CSARS a constaté que les enquêteurs du SCRS ne s'étaient pas prémunis de l'autorisation requise de la haute direction dans cette affaire et il a rappelé au Service son obligation de le faire.

Constatations

Le CSARS a constaté que les opérations du bureau régional du SCRS cadraient pleinement avec toutes les lois, instructions et politiques applicables. Le SCRS avait des motifs raisonnables de soupçonner que les cibles d'enquêtes autorisées dans cette région menaçaient la sécurité du Canada et le degré d'intrusion des méthodes employées allait de pair avec la présumée menace. Les informations recueillies par le SCRS lui étaient strictement nécessaires pour remplir son mandat. Le CSARS a constaté avec satisfaction que le personnel de ce bureau régional fait face aux nouvelles menaces en temps utile et de façon professionnelle.

Le bureau régional a respecté toutes les exigences de la Cour fédérale du Canada dans ses demandes de mandats et dans l'exercice des pouvoirs conférés par ceux-ci lors d'enquêtes particulières. De plus, le Service a agi de façon irréprochable et respectueuse de la loi dans sa gestion des sources humaines. Le CSARS a relevé quelques erreurs administratives dans certains dossiers de sources humaines, mais il les a considérées comme mineures et sans incidence sur les enquêtes du Service.

La coopération du bureau régional, ses échanges d'information avec les partenaires canadiens et l'application des politiques, pratiques et procédures relatives à la sécurité n'ont suscité aucune préoccupation au CSARS.

Cette étude n'a donné lieu à aucune recommandation.

Étude d'une enquête antiterroriste

Étude n° 2006-03

Contexte

Cette étude a gravité autour d'une enquête menée à l'échelle nationale par le SCRS sur deux organisations du Moyen-Orient qui étaient inscrites à titre d'entités terroristes en vertu du *Code criminel* du Canada. L'objectif du Service était de découvrir s'il y avait une présence officielle de ces groupes terroristes au Canada et d'identifier les réseaux de soutien ainsi que les personnes ou les groupes qui étaient associés à ces organisations au Canada.

Même s'il s'agit là d'une enquête relativement longue, elle n'a jamais comploté plus de dix cibles autorisées, pendant la période considérée, soit du 1^{er} septembre 2002 au 30 novembre 2005. À la fin de 2005, le SCRS n'avait décelé aucune présence structurée de ces groupes qui soit officielle au Canada, mais il avait ouvert plusieurs enquêtes nouvelles sur des personnes qui, croyait-on, étaient liées aux organisations visées par l'enquête ou agissaient en leur nom.

De plus, une nouvelle entente avait été conclue en vertu de l'article 17, avec un organisme de la région, conformément aux instructions ministérielles et à la politique opérationnelle. Tous les échanges d'information avec des organismes étrangers comportaient les mises en garde prescrites dans la politique opérationnelle, soit que le Service veille à ce que toute information transmise à des partenaires étrangers porte la mention de provenance du SCRS et comporte des restrictions sur l'utilisation à en faire. Enfin, le CSARS a confirmé que la mission s'était conformée à la directive du SCRS de ne fournir aucune information à un service de renseignement étranger particulier et de ne pas coopérer avec lui au cours de la période à l'étude à cause de craintes quant à la fiabilité de cet organisme.

Cette étude n'a donné lieu à aucune recommandation.

Étude des activités et enquêtes d'un bureau régional du SCRS

Étude n° 2006-02

Contexte

Le CSARS examine régulièrement les activités et enquêtes du SCRS dans chaque région du Canada, à tour de rôle. Ces études régionales permettent de voir de quelle manière les enquêtes autorisées par l'Administration centrale du SCRS sont menées en région. Elles aident en outre le CSARS à mieux connaître les priorités et les difficultés propres à chaque bureau régional.

Cette année, le CSARS a choisi d'examiner le plus petit bureau régional du SCRS. En dépit de sa taille, ce bureau a pleins pouvoirs opérationnels et administratifs.

Méthode

Pour la période du 1^{er} septembre 2004 au 31 août 2005, le CSARS a évalué les activités de ce bureau régional par rapport à la *Loi sur le SCRS*, aux instructions ministérielles et aux politiques opérationnelles. À ce bureau, le CSARS a examiné :

- le processus d'autorisation des enquêtes et la conduite de celles-ci contre les cibles;
- la demande et l'exercice de pouvoirs conférés par mandat et les opérations spéciales;
- le recrutement et l'essai de sources humaines et l'attribution de missions à celles-ci;
- la coopération, la liaison et les échanges d'information avec les partenaires canadiens;
- les mesures et la procédure de sécurité interne.

Examen d'un bureau de liaison-sécurité

Étude n° 2006-01

Contexte

Au cours de la période à l'étude, le SCRS avait, de par le monde, un certain nombre de bureaux d'agent de liaison-sécurité (ALS)¹ dont le nombre et l'emplACEMENT sont classifiés, mis à part ceux de Londres, Paris et Washington. Avec Citoyenneté et Immigration Canada, ces bureaux s'emploient à traiter les demandes d'immigration. De plus, ils échangent des renseignements en matière de sécurité, conseillent les cadres supérieurs de la mission ou de l'ambassade canadienne et assurent la liaison avec les services étrangers de renseignement de sécurité avec lesquels le Service a des ententes approuvées.

Méthode

Le CSARS a examiné la manière dont le Service avait géré ses relations avec ce bureau, et tous les échanges d'information avec les services étrangers de renseignement de sécurité concernés. Il s'est aussi penché sur la gestion du personnel affecté par le SCRS à la mission, et sur les visites dans la région ou sur celles du personnel qui y est affecté, et il a étudié les évaluations des organismes avec lesquels coopère l'ALS, un profil de la mission même ainsi que tous les rapports ou études du SCRS sur les pays qui entrent dans le champ de responsabilité de ce bureau. Le CSARS a notamment examiné l'impact des tâches de filtrage de sécurité à l'immigration sur les autres fonctions de l'ALS.

Constatations

Le CSARS a constaté que la mission était dirigée efficacement et que ses opérations étaient conformes à la *Loi sur le SCRS* et aux instructions ministérielles ainsi qu'à la politique opérationnelle et aux lignes directrices du SCRS. Le personnel de la mission remplissait et remettait régulièrement les formulaires de suivi de l'immigration et présentait tous les formulaires de contact et de visites requis. La mission fournissait en temps utile des renseignements et conseils pertinents concernant les visites de représentants étrangers à l'Administration centrale du SCRS. Les approbations requises ont été demandées et obtenues à l'égard de toutes les visites. Les évaluations que le SCRS a faites des organismes avec lesquels il coopère étaient, pour la plupart, exactes et présentées en temps opportun.

¹ Depuis lors, les ALS sont devenus des agents à l'étranger, dans le cadre de la réorganisation du SCRS. Voir les détails à la section 2.

Le programme de recherche du CSARS est conçu de manière à englober un vaste éventail de sujets. Lorsqu'il décide des études à mener, le Comité tient compte des éléments suivants :

- les événements susceptibles de susciter des menaces à la sécurité du Canada;
- les activités particulières qui pourraient porter atteinte aux droits et libertés individuels;
- le rapport annuel classifié, présenté au Ministre par le directeur du SCRS;
- la nécessité d'évaluer régulièrement chacune des directions opérationnelles du Service et chacun de ses bureaux régionaux;
- les pouvoirs que lui confère la *Loi sur le SCRS*, selon les détails qu'on y trouve;
- les priorités et préoccupations qui sont énoncées par le Parlement ou dans les médias;
- les engagements du CSARS à réexaminer des questions particulières;
- les questions cernées par le Comité dans l'exercice de ses fonctions relatives aux plaintes;
- les orientations stratégiques ou initiatives nouvelles annoncées par le SCRS ou par le gouvernement du Canada.

Cette approche permet au Comité de gérer le risque que comporte le fait de ne pouvoir examiner qu'un petit nombre des activités du SCRS une année donnée. Chaque étude est un « instantané » des actions du Service dans un contexte particulier. Depuis plus de deux décennies, les études du CSARS fournissent au Parlement et aux Canadiens un tableau complet des activités opérationnelles du Service et l'assurance que les actions de celui-ci sont conformes à la loi.

Le Comité n'est qu'un des divers mécanismes qui sont conçus pour assurer la reddition de comptes du SCRS. Celui-ci doit en outre faire rapport de ses opérations par l'entremise de l'appareil gouvernemental en place, notamment le ministre de la Sécurité publique, l'inspecteur général du SCRS, les organismes centraux et le vérificateur général ainsi que les commissaires à l'information et à la protection de la vie privée du Canada.

A. Examen des activités de renseignement de sécurité du SCRS

EXERCICE DE SA FONCTION DE SURVEILLANCE PAR LE CSARS

Le Comité de surveillance des activités de renseignement de sécurité est le seul organisme à être habilité par la loi et à avoir l'expertise voulue pour effectuer, de l'extérieur, un examen indépendant des activités du SCRS. Il a été créé en vertu de la *Loi sur le SCRS* (1984) afin d'assurer au Parlement du Canada et aux Canadiens que l'action du Service est conforme à la loi, aux politiques et aux instructions ministérielles dans l'exercice de ses fonctions. Ce faisant, le CSARS s'emploie à veiller à ce que le SCRS respecte les droits fondamentaux et les libertés des Canadiens.

Pour remplir son mandat, le Comité confie chaque année à son personnel diverses études qui fournissent un examen rétrospectif et une évaluation d'enquêtes et de fonctions particulières du SCRS. La *Loi sur le SCRS* lui confère des pouvoirs quasi illimités pour ce qui est de scurter le rendement du Service. Exception faite des seuls renseignements confidentiels du Cabinet, le CSARS a le pouvoir absolu d'examiner toute information touchant les activités du SCRS, quel qu'en soit le niveau de classification.

Le rapport de chaque étude contient des constatations et des recommandations du Comité. Une fois terminé, il est présenté au directeur et à l'inspecteur général du SCRS.

En vertu de l'article 54 de la *Loi sur le SCRS*, le CSARS est en outre autorisé à présenter au ministre de la Sécurité publique un rapport spécial sur toute question que ses membres estiment revêtir une importance particulière, ou tout rapport spécial que celui-ci lui demande.

En quoi un organisme de contrôle diffère-t-il d'un organisme surveillance?

Un organisme de contrôle suit en permanence ce qui se passe au sein d'un service de renseignement et il a pour mandat d'évaluer et de guider les enquêtes ou les travaux en cours « en temps réel ». Le CSARS est un organisme de surveillance de sorte que, contrairement à un organe de contrôle, il peut évaluer pleinement le rendement passé du SCRS, sans être mêlé d'aucune manière à ses décisions et activités courantes d'ordre opérationnel.

Bilan de l'exercice 2006-2007

Section 1

Le Comité de surveillance des activités de sécurité fournit au Parlement du Canada, et par son entremise aux Canadiens, l'assurance que le Service canadien du renseignement de sécurité (SCRS) respecte la loi dans l'exercice de ses fonctions. Le CSAFS a deux fonctions principales. La première consiste à mener des études approfondies sur les activités du Service pour vérifier si elles sont conformes à la *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*) et aux divers instruments stratégiques qui en découlent, ainsi qu'aux instructions du ministre de la Sécurité publique. La seconde consiste à recevoir les plaintes de quiconque à l'égard des activités du Service et à faire enquête à ce sujet.

Le Rapport annuel du CSAFS 2006-2007 est agencé en fonction des principales constatations et recommandations qui découlent de ses études et de ses enquêtes sur les plaintes. On y trouve aussi les renseignements plus généraux qu'il recueille pour informer ses membres et aider le lecteur à saisir le contexte plus vaste dans lequel baigne le travail de renseignement de sécurité du SCRS. Voici les trois sections de ce rapport :

Section 1 : Bilan de l'exercice 2006-2007

Cette section résume neuf études que le CSAFS a effectuées durant la période visée par le présent rapport. Elle fournit aussi de l'information sur cinq rapports de plaintes qu'il a remis.

Section 2 : Mécanismes redditionnels du SCRS

Cette section décrit le cadre de politiques et de régie à l'intérieur duquel fonctionne le SCRS. Elle expose aussi les renseignements que le Service fournit au sujet de ses activités, plans et priorités opérationnels, et cela, par rapport à ses principales directions.

Section 3 : Au sujet du CSAFS

Cette section fournit des détails sur les activités du Comité en matière de rayonnement, de liaison et d'administration, y compris sur son budget annuel et ses dépenses.

En examinant le rôle du SCRS dans cette affaire, nous avons conclu que quelques-unes de ses actions avaient violé certains droits garantis par la *Charte*. En conséquence, nous avons fait plusieurs recommandations au ministre de la Sécurité publique et au directeur du SCRS.

Il importe de comprendre pourquoi le CSARS s'inscrit en faux contre certaines actions du SCRS et nous invitons le lecteur à examiner notre analyse avec soin. Mohammed Mansour Jabarah est un Canadien qui, si haineux que soient ses crimes et si vifs que soient nos regrets face à ceux-ci, a qualité pour jouir de tous les droits et libertés qui sont reconnus à tout autre citoyen en vertu de notre *Charte*. De plus, un mandataire de l'État doit confirmer la *Charte*, sinon les représentants canadiens auraient toute latitude pour choisir à qui s'appliquent certains droits et libertés qui leur sont garantis. Cela serait nettement inacceptable pour tous les Canadiens.

Un mandataire de l'État doit confirmer la *Charte*, sinon les représentants canadiens auraient toute latitude pour choisir à qui s'appliquent certains droits et libertés qui leur sont garantis.

Le CSARS reconnaît que, dans la foulée du 11 septembre où se trouve notre monde, les services de police et de renseignement de sécurité doivent faire face à des défis intimidants, dont divers groupes terroristes mondialisés et astucieux sur le plan technique. Nous savons aussi que la sécurité relative dont jouissent les Canadiens, nous la devons en grande partie aux efforts déployés en notre nom par ces mêmes services. Mais l'obligation d'assurer la sécurité du public ne doit en aucune manière affaiblir le respect de la règle de droit.

Le juge Ian Binnie, de la Cour suprême du Canada, a qualifié de « combat de titans » les intérêts antagonistes de la sécurité nationale et des droits de la personne. Il est vrai que, parfois, les objectifs entourant les droits de la personne et la sécurité nationale peuvent sembler s'opposer. Mais, dans une démocratie saine au sein de laquelle les droits et les libertés sont protégés par la constitution, nous croyons fermement que ces intérêts peuvent et, en fait, doivent coexister. Voilà un principe que tous les Canadiens doivent confirmer et que tout citoyen a la responsabilité de protéger sans défaillance.

Déclaration du Comité

Cette année marque un anniversaire important dans l'histoire du Canada. Un quart de siècle s'est écoulé depuis l'adoption de la *Charte canadienne des droits et libertés*, qui garantit la liberté de conscience et de religion; la liberté de pensée, de croyance, d'opinion et d'expression, y compris la liberté de la presse; la liberté de réunion pacifique; et la liberté d'association. L'adoption de la *Charte* a permis de protéger ces libertés par la Constitution et de donner aux Canadiens un recours devant les tribunaux si l'État brime les droits que leur garantit la *Charte* ou y porte atteinte.

Il ne faut aucun doute que les valeurs fondamentales énoncées dans ce document constitutionnel historique ont aidé à définir ce que veut dire être Canadien. Elles ont eu une influence profonde sur le gouvernement, par exemple, sur les travaux d'organismes de surveillance tel le Comité de surveillance des activités de renseignement de sécurité (CSARS). Ces libertés ont été vivement mises en relief ces dernières années lorsqu'on les a mises en parallèle avec l'obligation de l'État d'assurer la sécurité de ses citoyens face à la montée de la menace terroriste.

Dans l'exercice de ses devoirs, le Comité en est souvent venu à scruter des questions entourant la *Charte*. Par exemple, dans le cadre de nos études, nous examinons régulièrement la manière dont le SCRS exerce les pouvoirs qui lui sont confiés par la voie de mandats judiciaires pour nous assurer que ses méthodes d'enquête intrusives respectent la loi et les conditions énoncées par le tribunal et ne constituent donc pas des perquisitions et des saisies à caractère abusif.

Le CSARS reconnaît que la conduite des services de renseignement de sécurité peut susciter un débat passionné quant à savoir si la fin peut jamais justifier les moyens. Il sait en outre de première main que des individus cherchent à profiter des droits et libertés du Canada pour porter préjudice à notre pays, à ses citoyens ainsi qu'à nos voisins et amis de par le monde.

C'est sur cette toile de fond que figure, dans le rapport annuel du CSARS, le résumé d'un rapport présenté le 17 août 2007 au ministre de la Sécurité publique, en vertu de l'article 54. Les rapports semblables sont relativement rares : il n'y en a eu que huit dans la dernière décennie. Ce dernier rapport traite de l'affaire Mohammed Mansour Jabarah, citoyen canadien et, de l'aveu de tous, membre d'Al-Qaïda, qui a été jugé coupable d'infractions liées au terrorisme aux États-Unis.

Section 2 : Mécanismes redditionnels du SCRS	33
A. Exigences en matière de rapports	35
Rapport annuel du directeur du SCRS (2005-2006)	35
Certificat de l'inspecteur général du SCRS (2006)	36
Agissements illicites du SCRS	38
Communication d'informations	38
B. Ententes avec des organismes canadiens et étrangers	39
Ententes avec des organismes canadiens	39
Ententes avec des organismes étrangers	39
C. Politiques et régie	41
Exigences nationales en matière de renseignement de sécurité	41
Instructions ministérielles	42
Modifications à la politique opérationnelle du SCRS	42
Règlements et nominations par le gouverneur en conseil	42
D. Activités opérationnelles du SCRS	43
1. Renseignement	44
Direction du filtrage de sécurité	44
Direction de l'évaluation du renseignement	44
Direction des sources humaines et du soutien aux opérations	50
Direction des services techniques et scientifiques	50
Centre intégré d'évaluation des menaces	51
2. Opérations	51
Direction du terrorisme international	51
Direction du Moyen-Orient et de l'Afrique	51
Direction de l'Asie, de l'Europe et des Amériques	52
Région internationale	52
Mandats de la Cour fédérale : généralités et statistiques	52
Section 3 : Au sujet du CSARS	55
Composition du Comité	57
Réunions et exposés du CSARS, 2006-2007	57
Personnel et organisation	58
Budget et dépenses	59
Demandes en vertu des Lois sur l'accès à l'information et sur la protection des renseignements personnels	59
Communications	60
Responsabilisation de gestion	60
Annexe A : Rapports et études du CSARS depuis 1984	63
Annexe B : Recommandations	77

Table des matières

Déclaration du Comité v

Agencement du rapport vii

Section 1 : Bilan de l'exercice 2006-2007 1

A. Examen des activités de renseignement de sécurité du SCRS 3

Exercice de sa fonction de surveillance par le CSARS 3

Examen d'un bureau de liaison-sécurité (2006-01) 5

Etude des activités et enquêtes d'un 6

bureau régional du SCRS (2006-02) 6

Etude d'une enquête antiterroriste (2006-03) 7

Etude d'une activité visée à l'article 16 (2006-04) 9

Etude d'une enquête antiterroriste (2006-05) 11

Etude de la collaboration et des échanges de 11

renseignements du SCRS à la suite du 11 septembre (2006-06) 12

Etude du filtrage de sécurité à l'extérieur 14

de l'administration fédérale (2006-07) 14

Etude n° 2006-08 16

Examen de l'Unité des enquêtes de 16

contre-espionnage du SCRS (2006-09) 16

B. Rapport en vertu de l'article 54 18

Etude de l'affaire Mohammed Mansour Jabarah (2005-05) 18

C. Enquêtes sur les plaintes 23

Procédure d'enquête du CSARS sur les plaintes 23

Détermination de la compétence du CSARS à examiner une plainte 26

D. Décisions du CSARS à l'égard des plaintes 2006-2007 27

Discrimination présumée dans un processus d'immigration (2006-01) 27

Présumées actions du SCRS lors d'une 28

entrevue de citoyenneté (2006-02) 28

Révocation d'une habilitation de sécurité (2006-03) 28

Prétendues fausses déclarations (2006-04) 30

Retard allégué à traiter une demande de citoyenneté (2006-05) 31


Le 28 septembre 2007

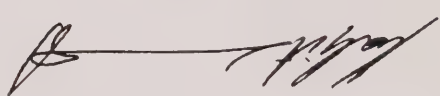
L'honorable Stockwell Day, C.P., député
Ministre de la Sécurité publique
Chambre des communes
Ottawa (Ontario)
K1A 0A6
Monsieur le Ministre,

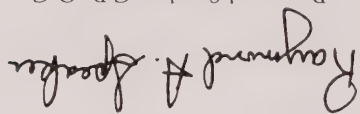
Conformément à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, nous présentons au Parlement, par votre entremise, le rapport du Comité de surveillance des activités de renseignement de sécurité pour l'exercice 2006-2007.

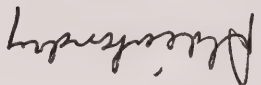
Veuillez agréer, Monsieur le Ministre, l'expression de notre haute considération.

Le Président,


Gary Filmon, C.P., O.M.


Baljit S. Chadha, C.P.


Raymond A. Specker, C.P., O.C.


Aldéa Landry, C.P., C.M., c.r.

Les membres du CSAFS (de gauche à droite) :
l'honorable Baljit S. Chadha, l'honorable Gary Filmon (président), l'honorable Raymond Speaker,
l'honorable Aldéa Landry et l'honorable Roy Romanow



Photo : Courrette/Ottawa

Examen opérationnel du Service
canadien du renseignement de sécurité

Rapport annuel du CSARS 2006-2007



Comité de surveillance des activités de renseignement de sécurité
B.P. 2430, succursale D
Ottawa (Ontario)
K1P 5W5

Téléphone : 613-990-8441

Télécopieur : 613-990-5230

www.sirc-csars.gc.ca

Les appels à frais virés sont acceptés de 8 h à 17 h, heure normale de l'Est.

Nota : aux fins du présent document, la forme masculine désigne, s'il y a lieu, aussi bien les femmes que les hommes.

© Travaux publics et Services gouvernementaux Canada 2007
N° de catalogue PS105-2007
ISBN 978-0-662-05006-3

Rapport annuel du CSARS 2006-2007

Examen opérationnel du Service
canadien du renseignement de sécurité





SECURITY INTELLIGENCE
REVIEW COMMITTEE

GOVT

CA1
SIR
- A56

SIRC Annual Report 2007–2008

An operational review of the
Canadian Security Intelligence Service



Security Intelligence Review Committee
P.O. Box 2430, Station "D"
Ottawa ON
K1P 5W5

(613) 990-8441

www.sirc-csars.gc.ca

Collect calls are accepted between 8:00 AM and 5:00 PM, EST

© Public Works and Government Services Canada 2008

Cat. No. PS105-2008

ISBN 978-0-662-05944-8



SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Annual Report 2007–2008

**An operational review of the
Canadian Security Intelligence Service**



Members of SIRC (from left to right):
The Honourable Baljit S. Chadha, The Honourable Gary Filmon (Chair), The Honourable
Raymond Speaker, The Honourable Aldéa Landry, The Honourable Roy Romanow

September 30, 2008

The Honourable Stockwell Day, P.C., M.P.
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6

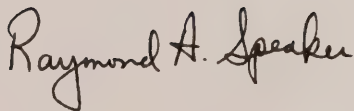
Dear Minister:

As required by Section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 2007–08, for your submission to Parliament.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Gary Filmon'.

Gary Filmon, P.C., O.M.
Chair

A handwritten signature in black ink, appearing to read 'Raymond A. Speaker'.

Raymond Speaker, P.C., O.C.

A handwritten signature in black ink, appearing to read 'Roy Romanow'.

Roy Romanow, P.C., O.C., Q.C.

Table of contents

Members' Statement	v
How this report is organized	vii
Section 1: A year in review 2007–08	1
A. Review of CSIS security intelligence activities	3
Review 2007-01: Review of CSIS's cooperation with and investigation of the intelligence agencies of a foreign country	5
Review 2007-02: Review of a counter-intelligence investigation	6
Review 2007-03: Review of CSIS's Intelligence Assessments Branch ..	8
Review 2007-04: Review of CSIS's support for Canadian operations abroad	9
Review 2007-05: Review of CSIS human source operations outside Canada	11
Review 2007-06: Review of a counter-terrorism investigation	12
Review 2007-07: Review of a Foreign Office	13
Review 2006-08: Review of a counter-terrorism investigation	15
B. Investigation of complaints	17
C. SIRC complaint decisions 2007–08	21
Report 2007-01: Alleged intimidation	21
Report 2007-02: Alleged abuse of human rights and unfair treatment	22
Report 2007-03: Allegations concerning CSIS's handling of evidence obtained by torture	22
Report 2007-04: Alleged discriminatory practice	25
Report 2007-05: Alleged improper advice to the Minister of Citizenship and Immigration	28
Report 2007-06: Alleged unreasonable delay in processing a site-access clearance	30

Section 2: CSIS operational activities and accountability mechanisms	33
A. CSIS operational activities	35
i. Intelligence	36
Security Screening Branch	36
Intelligence Assessments Branch	42
Human Sources and Operations Support Branch	43
Scientific and Technical Services Branch	43
Integrated Threat Assessment Centre	43
ii. Operations	44
Federal Court warrants and warrant statistics	45
B. Reporting requirements	46
CSIS Director's Annual Report (2006–07)	46
Certificate of the Inspector General of CSIS (2006–07)	47
Unlawful conduct by CSIS	47
Disclosure of information	48
C. Foreign and domestic arrangements	49
Arrangements with domestic agencies	49
Arrangements with foreign agencies	50
D. Policy and governance	51
National Requirements for Security Intelligence	51
Ministerial Direction	52
CSIS operational policy	52
Governor-In-Council regulations and appointments	52
Section 3: About SIRC	53
Committee membership	55
Staffing and organization	55
Committee activities	55
Budget and expenditures	56
Inquiries under the <i>Access to Information Act</i> and the <i>Privacy Act</i>	57
Summary of SIRC recommendations concerning reviews	61
Summary of SIRC recommendations concerning complaints	63

Members' Statement

For more than two decades, the Security Intelligence Review Committee (SIRC) has served to reassure Parliament and through it, Canadians, that the Canadian Security Intelligence Service (CSIS) is exercising its mandate to protect Canada's national security effectively and appropriately. In recent years, amidst dramatic changes to the nature and scope of the security intelligence landscape, SIRC's accountability function has taken on increasing significance. Unlike the Cold War era when there was a clear demarcation of interests between Western and Communist states, threats to national security today are much more diffuse and complex—transcending traditional state, political and geographic boundaries. The phenomena of transnational and homegrown terrorism are two such examples of this changing security environment. In response to this still-evolving context, most western nations, including Canada, have implemented fundamental changes to the ways in which they approach terrorism issues.

This transition has underscored the importance of independent, expert and informed review of CSIS. Whether in response to new legislative measures, changes to the security certificate process, various court decisions, findings from public inquiries or increased demands from government for security intelligence assessments, CSIS has implemented significant adjustments to its intelligence collection priorities and methods. SIRC has worked diligently to understand and evaluate these transformations, while ensuring that CSIS acts appropriately, effectively and in accordance with the law. Our reviews and complaint decisions provide an important means to reassure Canadians that CSIS continues to investigate new and evolving threats to national security in a manner that respects Canada's core democratic values. We accept this responsibility with an enormous sense of pride and probity.

With virtually unlimited access to all information under the control of CSIS—Cabinet confidences being the sole exception—SIRC is also uniquely situated to provide context to the debates about the nature and scope of the threat environment, and how these are addressed. Although SIRC does not promote any particular viewpoint or policy perspective, our reviews and complaint decisions provide important snapshots of CSIS's work—offering examinations of the nature and extent of the threat environment, and whether the Service addresses these threats appropriately and effectively and in a manner that respects its powers and authorities.

It is our hope that the declassified review summaries and complaints decisions that are published in our annual reports can help to inform ongoing public debate about the role of CSIS in protecting Canada's national security.

“With the *Canadian Charter of Rights and Freedoms* coming into play more often in matters of national security, and the advent of the newly created special advocate process, the guidance of the courts is both important and necessary if we, as a nation, are to find and preserve the right balance between national security and individual rights.”

Readers of this year's annual report will note that in two of SIRC's decisions in complaints during 2007–08, SIRC recommended that CSIS amend its policy of destroying operational notes and, instead, retain those notes. These recommendations echoed our earlier recommendations and were aimed at ensuring that complainants and SIRC, as a quasi-judicial body, would have full access to all information relevant to matters brought before the Committee for a determination.

We are pleased that the Supreme Court of Canada's recent decision in *Charkaoui vs. Canada (Citizenship and Immigration)*, 2008 SCC 38, has brought clarity to this issue and that the court's decision reflects SIRC's oft-stated views on the matter.

With the *Canadian Charter of Rights and Freedoms* coming into play more often in matters of national security, and the advent of the newly created special advocate process, the guidance of the courts is both important and necessary if we, as a nation, are to find and preserve the right balance between national security and individual rights.

SIRC strives to bring a fair and balanced perspective to our examinations of CSIS's performance. Although the Committee recognizes the increasing complexity and challenges in CSIS's work, we are always mindful of the high standards of accountability that are

essential for the legitimacy of a security intelligence agency in a democratic society. This means that, at times, SIRC will be critical of how CSIS performs, but it also means we will applaud, when warranted, the Service's contributions to protecting Canada's security. At all times we will endeavour to stay true to our commitment to earn and maintain the trust of the Canadian public in fulfilling the role that Parliament has entrusted to us.

How this report is organized

The Security Intelligence Review Committee's annual report has three sections.

Section 1: A year in review 2007–08

This section summarizes the reviews completed by SIRC as well as the complaint reports issued by SIRC during the period covered by this report.

Section 2: CSIS operational activities and accountability mechanisms

Featured in this section is information provided by CSIS on operational activities, plans and priorities, organized according to the Service's major branches. This section also contains descriptions of the policy and governance framework within which CSIS operates.

Section 3: About SIRC

This section provides details about the outreach, liaison and administrative activities of SIRC, including its annual budget and expenditures.

Section 1

A year in review 2007–08

A. Review of CSIS security intelligence activities

HOW SIRC CARRIES OUT ITS REVIEW FUNCTION

The Security Intelligence Review Committee (SIRC) was created in 1984 as the only body with a mandate to carry out ongoing, independent review of the activities of CSIS.

Established under the *CSIS Act*, SIRC provides assurance to Parliament—and through it, to Canadians—that CSIS performs its duties and functions appropriately and effectively and in accordance with legislation, policy and Ministerial Direction. In doing so, SIRC seeks to ensure that CSIS both protects and respects the fundamental rights and freedoms of Canadians.

To fulfill its mandate, SIRC directs staff to undertake a number of reviews each year. These provide a retrospective examination and assessment of specific CSIS investigations and functions. Under the *CSIS Act*, SIRC has virtually unlimited power to review CSIS's performance. With the sole exception of Cabinet confidences, SIRC has the right to have access to any information under the control of the Service, no matter how highly classified that information may be.

SIRC's reviews include findings and, where applicable, recommendations. Upon completion, the report is forwarded to both the Director of CSIS and the Inspector General of CSIS. SIRC is also authorized under Section 54 of the *CSIS Act* to provide special reports to the Minister of Public Safety on any matter that the Committee identifies as having special importance or that the Minister directs SIRC to undertake.

What's the difference between an oversight and a review agency?

An oversight body looks on a continual basis at what is taking place inside an intelligence service and has the mandate to evaluate and guide current investigations or work in "real time." SIRC is a review body, so unlike an oversight agency, it can make a full assessment of CSIS's past performance without being compromised by any involvement in its day-to-day operational decisions and activities.

SIRC's research program is designed to address a broad range of subjects. In deciding what to review, SIRC considers:

- events with the potential to represent threats to the security of Canada;
- particular activities by CSIS that could intrude on individual rights and freedoms;
- the CSIS Director's annual classified report to the Minister;
- the need to assess regularly each of the Service's branches and regional offices;
- SIRC's statutory authorities as detailed in the *CSIS Act*;
- priorities and concerns identified by Parliament or in the media;
- commitments by SIRC to re-examine specific matters;
- issues identified in the course of SIRC's complaints functions; and
- new policy directions or initiatives announced by CSIS or the Government of Canada.

This approach allows SIRC to manage the inherent risk of being able to review only a small number of CSIS activities in any given year. Each review results in a "snapshot" of the Service's actions in a particular context. For more than twenty years, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities, and assurance that CSIS is performing its duties and functions appropriately, effectively and in accordance with the law.

For each review, SIRC's researchers will consult multiple information sources to examine specific aspects of the Service's work. For example, in addition to consulting the academic literature and arranging briefings with CSIS employees, researchers will spend considerable time reviewing various documents at CSIS headquarters. As part of this process, researchers may look at individual- and group-targeting files, human source files, operational messages and other relevant correspondence, documents relating to cooperation between CSIS and foreign and domestic agencies and partners, intelligence assessments and warrant documents, among other sources that vary between reviews. The goal is to create a diverse pool of information so SIRC can ensure that it has thoroughly reviewed, and completely understood, the issues at hand. SIRC is pleased that CSIS has made every effort to facilitate and improve SIRC's access to these information sources, and we appreciate their efforts in this regard.

SIRC is only one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through the existing apparatus of government, specifically the Minister of Public Safety, the Inspector General of CSIS, the central agencies, the Auditor General, the Information Commissioner and the Privacy Commissioner of Canada.

SIRC REVIEWS IN 2007–08

Review of CSIS's cooperation with and investigation of the intelligence agencies of a foreign country

Review 2007-01

Background

Traditionally, counter-intelligence investigations conducted by CSIS have focused on countries operating covertly in Canada. In this case the Service both cooperated with and investigated the intelligence agencies of a foreign country. SIRC was interested in examining the challenges faced by CSIS in managing these relationships, while also guarding against suspected threat-related activities. SIRC also examined whether the information exchanged and the cooperation undertaken with these agencies were within the scope of the relevant foreign arrangements, as well as whether there were any problems or issues that arose from this situation.

Findings

SIRC found that, despite greater cooperation between CSIS and the targeted agencies, the Service clearly had a legitimate interest in investigating the covert activities of those agencies. Although any relationship in these circumstances has the potential to become conflicted, SIRC assessed that CSIS handled its investigation in an effective manner. At the same time, SIRC confirmed that the Service needed to continue to exercise both caution and balance in maintaining this relationship to ensure the protection of Canada's security interests. SIRC also found that CSIS employees did not always submit a contact or visit form, as required by operational policy, following contact with a foreign agency representative.

SIRC made two recommendations arising from this review.

First, SIRC recommended that CSIS employees submit a standard, written record of non-operational information exchanged with foreign agencies. This would be placed in both the relevant "cooperation with" file and operational database. The written record of non-operational information exchanged should also cross-reference the operational information exchanged with those foreign agencies. SIRC believes that as the number of visits with foreign agency representatives increases, it is important that CSIS employees be kept abreast of information exchanged with foreign agencies, so that they can get quick, comprehensive snapshots of these interactions.

Second, Section 17(1)(b) of the *CSIS Act* states that the Service may, with the approval of the Minister, “enter into an arrangement or otherwise cooperate” with foreign security or intelligence organizations, which is reiterated in Ministerial Direction and operational policy. During its review, SIRC found documents indicating that the Service was cooperating with a foreign agency with which it did not have a Section 17 arrangement. CSIS maintained that the information exchanged with that agency was covered by existing arrangements with other agencies in that country. Nevertheless, SIRC recommended that CSIS establish a separate Section 17 foreign arrangement with that agency to conform with the *CSIS Act*, Ministerial Direction and operational policy.

Review of a counter-intelligence investigation

Review 2007-02

Background

In this study, SIRC reviewed one of CSIS’s highest priority counter-intelligence investigations. This foreign intelligence service has conducted aggressive operations in Canada, targeting economic, political, scientific and technical information. It also has conducted operations against Canadian diplomatic premises and Canadian staff working overseas.

The objective of SIRC’s review was to assess CSIS’s performance in countering the foreign intelligence service’s attempts to cultivate sources of information within the Government of Canada, as well as its attempts to obtain surreptitiously economic intelligence and controlled technologies from Canadian businesses.

Findings

SIRC concluded that CSIS’s investigation was run professionally and was indicative of both strong operational planning and extensive experience with the investigation. The Service showed itself to be well positioned to identify and counter new threats posed by this foreign intelligence service. SIRC noted that CSIS had recently reconsidered and refocused its intelligence efforts to respond to a detected shift in practices by the foreign service in question. The Service must continue to shape its investigation to offset the challenges identified in this study and to close existing intelligence gaps.

SIRC also noted an inconsistent application of procedures for secure meetings with human sources, and expressed concern that certain practices could risk the security of CSIS’s operations and increase the chance of exposing the source’s relationship with the Service. As a result, SIRC suggested that CSIS review its practices and implement a consistent approach to all domestic human source operations.

An investigation of security concerns reported under the Government Security Policy

As part of this review, SIRC identified and reviewed CSIS's role in the investigation of security concerns that arose during the construction of the Department of National Defence's Above Ground Complex in North Bay, Ontario, as part of its North American Aerospace Defense Command (NORAD) modernization program. Although these issues were the subject of two reports by the Office of the Auditor General of Canada (May and October 2007), neither report discussed CSIS's role in the matter.

The Department of National Defence is responsible for meeting its security obligations under the Government Security Policy as they relate to the construction of this facility, and must report any concerns to CSIS when they arise. Further, CSIS is responsible for investigating national security concerns when they are reported. In this case, DND reported its security concerns to CSIS, and the Service responded in due course. SIRC noted, however, that CSIS did not receive sufficient information from the Department of National Defence to investigate various security concerns related to the NORAD facility fully and proactively.

SIRC also identified a gap in Canada's national security policy. The Government Security Policy requires all departments to request and receive security clearances from CSIS for individuals who require site access to secure facilities. The two reports issued by the Auditor General in 2007 indicated that departments and agencies often do not obtain the necessary security assessments for contractors. Yet there is no mechanism to alert CSIS when a department or agency has failed to meet these requirements.

SIRC believes that the failure of a department to request and receive appropriate security clearances could create a situation that could be exploited by a foreign intelligence service. Therefore, SIRC suggested that CSIS make every effort to be aware of construction projects involving secure locations and to develop a standardized procedure for CSIS to advise departments concerning the necessity of site access or security clearances.

SIRC recommended that CSIS consult with the Treasury Board Secretariat to clarify its responsibility to investigate incidents reported under the Government Security Policy, and to explore the value of enhancing interdepartmental liaison in order to advise departments of their security screening responsibilities under the policy. SIRC encourages CSIS to consider this recommendation as part of its future planning, and to include it in any discussions with the Treasury Board Secretariat about CSIS's responsibilities under the Government Security Policy.

Review of CSIS's Intelligence Assessments Branch

Review 2007-03

Background

CSIS's Intelligence Assessments Branch (IAB), formerly Research, Analysis and Production, plays an important role in providing timely and relevant strategic and tactical advice to the federal government concerning threats to national security. The IAB develops strategic analyses that examine current and emerging trends or issues that might affect national security in the future. The analyses are done for government or in support of Service investigations. It also prepares tactical analyses that support operational needs, including information about particular individuals, targets or other immediately pressing issues.

SIRC chose to review the IAB to enhance its understanding of the nature, scope and effectiveness of the branch's work. In addition to analyzing the strategic and tactical intelligence analyses produced by the branch, SIRC explored the nature and extent of the IAB's integration and cooperation with the wider Canadian security intelligence community and examined how the branch disseminated timely and relevant intelligence products.

Findings

Overall, SIRC found the IAB to be an effective and professionally organized group that has worked diligently in recent years to respond to growing demands—both within the Service and across government—for intelligence assessments and products. At the same time, considerable work remains for the IAB to adjust to the complex and changing security intelligence environment. This was recognized by IAB management and was demonstrated in ongoing work to improve and expand the branch's role. SIRC's review provided several insights into this ongoing transition.

First, recent organizational changes within the IAB should help to enhance the branch's capacity to produce strategic and tactical intelligence analyses for government or in support of Service investigations. In particular, SIRC believes that these changes represent an important step towards addressing the need for more long-term strategic analysis, especially since previous SIRC studies noted that frequent restructuring and insufficient resources had limited the Service's strategic intelligence assessment capabilities. For this reason, SIRC encourages CSIS's senior management to provide the necessary leadership and resources to ensure that the branch has the organizational stability to complete its important initiatives and objectives.

Second, SIRC believes that there will be increased pressure from across the security intelligence community for the IAB's assessments and related products. The challenge will be for the Service, and the IAB in particular, to continue to develop the capacity to meet those needs.

Third, SIRC found that the IAB has had a growing and important role collaborating with others in the Canadian intelligence community. For example, at an informal level, IAB analysts maintain contact across the intelligence community on a regular basis to share ideas and intelligence information. At a more formal level, these analysts and senior management participate in various interdepartmental working groups. SIRC believes that the branch's ongoing participation in such initiatives is essential in today's complex and evolving security environment.

SIRC's review also highlighted various challenges for the IAB in disseminating products and collecting client feedback. SIRC recognizes the Service's efforts to improve its methods of liaising with clients, to ensure that they receive relevant and timely analysis and commentary.

Review of CSIS's support for Canadian operations abroad

Review 2007-04

Background

The Director of CSIS noted in his 2006 speech to the Canadian Association for Security and Intelligence Studies that Canada's borders cannot protect the country from many of the threats it now faces. Canadian lives and property are at risk from the actions of individuals and groups residing in foreign countries—as are Canadians working or travelling abroad. In view of this, the Director maintained that one of CSIS's top challenges is “to strengthen (its) capacity to operate effectively outside of Canada in support of (its) core national security mandate.”

SIRC's review sought to examine the Service's efforts to increase its capacity to operate outside Canada. SIRC therefore analyzed, as a case study, CSIS's role in interdepartmental efforts abroad to rescue members of a group known as the Christian Peacemakers, who were kidnapped in Iraq in 2005.

The following questions guided SIRC's research:

- Is existing Ministerial Direction and policy guidance adequate in light of the changing nature of CSIS operations?
- Are there any specific lessons that CSIS can draw from its participation in interdepartmental initiatives abroad?
- As CSIS expands its capacity to operate abroad, how is it interacting with federal departments and agencies that also have an international presence?

Findings

SIRC found that CSIS officers increased in two ways the effectiveness of interdepartmental efforts to rescue the kidnapped members of the Christian Peacemakers. First, the officers provided access to information and priorities of other intelligence agencies operating in Iraq. Second, they provided information collected by human sources operating in the region.

At the same time, SIRC found that the Christian Peacemakers example illustrated the challenges that CSIS will face as it increases its activities abroad:

- Existing Ministerial Direction may need to be updated to provide CSIS with appropriate guidance.
- The speed with which the Christian Peacemakers crisis developed demonstrated the importance of advance preparations in terms of materiel and logistics as well as applicable policy guidance. CSIS's International Region has started work on developing a materiel and policy infrastructure to respond to such crises.
- The rescue operation demonstrated a need to conduct operational assessments, including communications, on a regular basis. SIRC noted two instances in which information was not communicated effectively, although there was no evidence that this affected the overall quality of the operation. CSIS informed SIRC that based on lessons learned overseas, changes were recommended to existing policies and that new procedures are being developed and implemented on an ongoing basis.
- The operation revealed the challenges that CSIS may face in conducting human source operations overseas. SIRC does understand that an assessment of risk may change with time, and that an operation may appear more or less risky in hindsight. Nonetheless, given the probability that the Service may be involved in the type of human source operations examined in this review, SIRC recommended that CSIS review the criteria used to conduct risk assessments, and that the Service define more precisely the high-risk situations for which it is necessary to consult with the Minister of Public Safety.

Review of CSIS human source operations outside Canada

Review 2007-05

Background

The complexities of dealing with human beings, and human relations, make human sources a unique and challenging line of intelligence collection. Nevertheless, human sources remain an essential tool in security intelligence for understanding both threat environments and the intentions of targets—information that is not always evident from technical sources such as photographs or intercepted communications.

SIRC examined the challenges of conducting human source operations overseas, including operations in war zones. SIRC assessed the Service's actions against the *CSIS Act* and Ministerial Direction, as well as relevant operational policies and guidelines. Special attention was given to whether current Ministerial Direction was sufficient to accommodate the Service's foreign collection activities and support for military operations.

Findings

SIRC believes that the expansion of CSIS's foreign intelligence collection program will entail challenges as the organization adapts to new operational environments. SIRC recognizes the Service's efforts to work effectively in this still-evolving context, evidenced by the creation of the International Region, which includes the transition from Security Liaison Officer to Foreign Officer, and the approval of Executive Directives to guide certain operations. However, further work remains to be done.

SIRC therefore made two recommendations. First, SIRC's analysis suggests that the Service should reconsider its policy structure to accommodate its increasing activities outside Canada. Although the Committee found that CSIS had revised its practices to meet the challenges identified in the study, corresponding Service policy has yet to be adjusted. SIRC believes it appropriate for the Service to extract common principles and themes from its current practices to develop new policy to govern overseas source operations. To be effective, these changes in policy should be led by the Minister of Public Safety by way of clear Ministerial Direction. SIRC therefore recommended that CSIS prioritize the development of these policies upon receipt of the new Ministerial Direction.

SIRC's second recommendation concerned the assessment of risk for source operations. When risk assessments were reported in the planning documentation reviewed, there was little detail as to how these assessments were calculated, and

little consistency in the language used. As a result, it was often unclear what factors motivated the assessment of a particular risk level. CSIS policy has neither a standardized scale establishing thresholds between different levels of risk, nor consistent terminology when assessing risk.

SIRC concluded that CSIS should rationalize its risk assessment procedures and its reporting of risk in operational plans. Clearly described standards would provide operational staff with a tool to measure and assess risk, and ensure that all factors are considered. SIRC therefore recommended that CSIS standardize its risk assessments with detailed and consistent terminology that is reflected in operational policy.

Review of a counter-terrorism investigation

Review 2007-06

Background

This review examined one of CSIS's largest and highest-priority investigations. Operational activity undertaken within this investigation had taken place both in Canada and abroad, and the Service had cooperated with allied intelligence agencies to disrupt certain threat-related activities.

In the period under review, SIRC examined the nature and extent of the activities of a sample of group and individual targets, including how these targets constituted a threat to the security of Canada, as well as the effectiveness and appropriateness of the Service's investigation.

Findings

Two findings and one recommendation resulted from this review.

One of the groups reviewed was approved as a target in 2004, and again in 2006. SIRC found that the Service had no indication that members of the targeted group had been directly involved in any terror-related acts. According to CSIS, its main concern was that these individuals could be regarded as ideal recruits by terrorist groups.

Although there is evidence to suggest that this group is a terrorist organization—for example, some of its members are thought to have participated in terrorist activities outside of Canada—there is also a wide body of academic literature that suggests it is non-violent, and has been targeted by a number of foreign governments because it is considered a political threat. Although SIRC's review noted that the Service, in its investigation, was aware of the debate regarding the group's status as a terrorist organization, there was no reference to that debate in the targeting approval

process. Therefore, SIRC's first finding was that this debate should have been included in the targeting approval process.

SIRC therefore recommended that the debate about whether the targeted group is in fact a terrorist organization should be included in future targeting discussions. Although the ensuing discussion might not alter the final decision, the targeting approval process would nonetheless be better informed.

Another aspect of the review included an examination of the Service's investigation of targets in sensitive Canadian institutions, which includes academic, political, media, religious and trade union fields. Ministerial Direction and operational policy require that CSIS obtain a higher level of approval prior to undertaking investigative activities that have an impact, or appear to have an impact, on these institutions. SIRC's second finding was that CSIS may be required to undertake certain types of investigative activities that could have an impact on a sensitive sector institution. SIRC therefore believes the Service should re-examine existing policies to ensure that these activities are suitably covered.

Review of a Foreign Office

Review 2007-07

Background

Because the vast majority of threats that CSIS must contend with arise beyond Canada's borders, the Service has taken steps to strengthen its capacity to operate effectively abroad. CSIS has for many years operated Foreign Offices around the world—the number and locations of which are classified, except for those in London, Paris and Washington. Service representatives working at these posts are designated Foreign Officers (FO), formerly Security Liaison Officers (SLO).

SIRC's review of one such Foreign Office was designed:

- to examine the nature and volume of the Foreign Office's immigration-related work and how other responsibilities (i.e., intelligence gathering and liaison) were balanced;
- to study the office's relationships with other Canadian agencies located in the host country;
- to analyze the office's liaison relationships with foreign agencies to ensure that CSIS was prudent in its dealings with those intelligence entities with questionable human rights practices; and
- to inquire how CSIS's 2006 reorganization affected work at the office.

Findings

SIRC's examination of this Foreign Office illustrated the challenges facing CSIS in an immigration-generating, geo-politically complex and threat-diverse region. The Service places high expectations on Foreign Officers to address these competing demands, requiring solid time management and the effective development of diverse information sources. SIRC noted the Foreign Officer's capable handling of these divergent expectations at the office.

From SIRC's perspective, two overlapping issues converged at this office: strategic restructuring challenges and tactical workload expectations. These issues will become particularly relevant for this Foreign Office as the region's security intelligence demands continue to evolve. The challenge for CSIS will be to balance expanding collection demands with resource realities.

SIRC offered three concluding observations for the Service to consider as it attempts to address these competing priorities. First, CSIS will need to acknowledge and address ongoing human resource capacity issues, particularly in relation to the increased workload demands related to the transition from Service Liaison Officer to Foreign Officer. Efforts at addressing this challenge will depend on the extent to which the Service perceives the need to bolster collection capabilities at the office. Second, SIRC encouraged the Service to continue with efforts to increase liaisons with partner agencies, a strategy that SIRC believes will offset the over-reliance on particular information sources. Third, SIRC encouraged CSIS to continue refining its plans and priorities that focus on threats originating outside Canada.

Considering that the Service's reorganization remains a work in progress, there were no recommendations arising from this review.

Review of a counter-terrorism investigation*

Review 2006-08

***Note:**

This review was not finalized until after the 2006–07 annual report went to print.

Background

Western-based intelligence agencies have noted in recent years the activities of certain Islamist-based movements around the world whose adherents employ violence against those declared to be “enemies of Islam.” In Canada, there are increasing concerns about the emergence of “homegrown” terrorist threats posed by so-called second generation Islamists—individuals born or raised in Canada who subsequently espouse radical beliefs, as well as converts who espouse extremist interpretations of Islam. CSIS has identified al Qaida-inspired threats as prominent, and particularly the threat posed by individuals who may, to all appearances, have blended into society.

To understand better why some who are born and raised in Canada might turn to extremism, and to prevent those who do so from engaging in threat-related activities, CSIS assigns priority to identifying the factors that may lead to radicalization.

SIRC reviewed the Service’s investigation of certain individuals believed to be second-generation terrorists or recent converts to extremist interpretations of Islam. SIRC also reviewed CSIS’s execution of warrant powers and its use of human sources.

Findings

SIRC found that the Service complied with the *CSIS Act*, as well as applicable Ministerial Direction and operational policies in this investigation. Specifically, SIRC found no issues of concern in CSIS’s examination of individual targets, the development and execution of a warrant, and the management and control of most of the human sources associated with this investigation.

Concerning CSIS’s direction of human sources, SIRC noted that appropriate authorization had not been provided by CSIS’s executive for operations conducted within sensitive institutions, as required by its sensitive-sector policy.¹ For instance, SIRC found that a regional investigator had directed a human source to collect information within a sensitive institution without first obtaining executive approval.

¹ Sensitive institutions include those in the academic, political, media, religious and trade union fields.

SIRC also found that the investigation's targeting-approval documentation did not provide a sufficiently thorough overview of the issue, group, organization or individual targeted or a description of the activities of the proposed target, as per operational policy. In particular, SIRC believes the documentation could have included more detail regarding how the investigation would focus on issues of new, evolving or increasing concern. In the absence of this information, the investigation has served as a general operational file for the broader investigation of Islamist extremism. SIRC believes that clarifying and limiting this issue-based investigation could assist CSIS in more effectively identifying issues of developing concern and isolating them for analysis.

Therefore, the Committee recommended that CSIS clearly define this issue-based investigation when it is next renewed and determine whether it should focus on issues of increasing concern.

B. Investigation of complaints

HOW SIRC INVESTIGATES COMPLAINTS

In addition to its review function, SIRC is responsible for investigating complaints about CSIS. SIRC is committed to listening and responding to Canadians, as this is one of the key roles entrusted to SIRC by Parliament. The Committee considers complaints made by citizens concerning any activity of CSIS, or in cases where a security clearance necessary to obtain or maintain federal government employment or contracts has either been denied or revoked. Almost all complaint cases begin as inquiries to SIRC, and SIRC staff make every effort to respond promptly to such inquiries, and inform prospective complainants about what the *CSIS Act* requires to pursue a complaint.

Once a written complaint is received, SIRC conducts an initial review. Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated. If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee members, assisted by staff.

In investigating complaints, SIRC has all of the powers of a superior court, and has access to all information in the possession of CSIS, except for Cabinet confidences. A complainant has the right to be represented by counsel and to make representations at the hearing. Pre-hearings may be conducted to establish and agree on procedures with the complainant and/or the complainant's counsel.

Types of complaints

Four kinds of matters may be investigated by SIRC:

- Complaints lodged by persons “with respect to any act or thing done by the Service” (Section 41);
- Complaints concerning denials of security clearances to government employees or contractors (Section 42);
- Referrals from the Canadian Human Rights Commission of allegations made to it; and
- Minister's reports in regards to the *Citizenship Act*.

SIRC's legal team provides advice on procedural and substantive matters, and will also cross-examine Service witnesses when, for national security reasons, evidence must be heard without the complainant being present.

COMPLAINTS CAN TAKE SEVERAL FORMS

The types of complaints that SIRC investigates are described in the *CSIS Act* and take several forms. Under Section 41 of the *CSIS Act*, SIRC can investigate “any act or thing” done by the Service. Under Section 42, it can hear complaints about denials of security clearances to federal government employees and contractors. Section 42 does not permit SIRC to accept jurisdiction to hear complaints concerning less intrusive background screening or reliability checks, which are conducted simply to determine the trustworthiness or suitability of a potential federal employee. These complaints are addressed through an organization's designated grievance procedure.

Pursuant to Section 42 of the *CSIS Act*, individuals who have been denied a security clearance must be informed of this action by the Deputy Head of the organization. These individuals have the right to make a complaint to SIRC and, where appropriate, SIRC will investigate and report its findings and any recommendations to the Minister, the Director of CSIS, the Deputy Head concerned and the complainant.

Should the Canadian Human Rights Commission receive a written notice from a Minister of the Crown about a complaint that relates to the security of Canada, the Commission may refer the matter to SIRC. Upon receipt of such a referral, SIRC carries out an investigation and reports its findings to the Commission, the Director of CSIS, the Minister of Public Safety, the Minister of the department concerned and the complainant. SIRC also has the authority to conduct investigations into matters referred to SIRC pursuant to the *Citizenship Act*.

When SIRC's investigation of a complaint made under Section 41 is concluded, it provides the Director of CSIS, the Minister of Public Safety and the complainant with a report of its findings and recommendations.² Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC's annual report to Parliament.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC's jurisdiction or investigated and resolved without a hearing (i.e., administrative review).

² The complainant receives a declassified version of the report.

Table 1
Resolution of complaints

	2005–06	2006–07	2007–08
Carried over	18	24	20
New	45	37	32
Total	63	61	52
Closed	39	41	37
Carried forward to subsequent year	24	20	15
Reports issued	4	5	6

How SIRC determines jurisdiction of a complaint...

...under Section 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by “any person” with respect to “any act or thing done by the Service.” Before SIRC investigates, two conditions must be met:

1. The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act*.

...under Section 42

With respect to security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

1. Any person refused federal employment because of the denial of a security clearance;
2. Any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
3. Anyone refused a contract to supply goods or services to the government for the same reason.

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

C. SIRC complaint decisions 2007–08

Alleged intimidation

Report 2007-01

SIRC reported a decision made under Section 41 of the *CSIS Act* about a complaint concerning the conduct of three male CSIS officers during their interaction with the complainant, a female lawyer. She alleged that the three men had addressed her in a physically threatening manner and intimidated her in the presence of her clients at an office of Citizenship and Immigration Canada (CIC). The complainant's clients, a husband and wife, required a security screening interview by CSIS for purposes of their application for permanent residence.

Without notice to the complainant, CIC scheduled the clients to each be interviewed by CSIS officers separately and simultaneously. According to the complainant, this scheduling meant that she could not be present with her clients at both interviews. A conflict arose between the complainant and the three CSIS officers over the scheduling of the interviews and the complainant's role during the interview. The complainant stated that she felt physically threatened by the CSIS officers and was shaking. She also found their behaviour and comments to be rude and sexist. Furthermore, she alleged that the CSIS officers were racist.

As part of SIRC's investigation, a hearing was held. The complainant did not offer an independent third party to testify about the alleged conduct of the CSIS officers. SIRC was left with two different but equally plausible interpretations of how the events transpired.

SIRC found that the three CSIS officers reacted reasonably under the circumstances. They were following CSIS policy concerning the conduct of immigration interviews. The three CSIS officers maintained that their conduct was not intended to intimidate, but rather to find out what the problem was regarding the scheduled interviews. The prospect of simultaneous interviews caused conflict for the complainant, while the prospect of re-scheduling consecutive interviews caused conflict for CSIS.

SIRC found that, given the circumstances of this case, both sides would have been agitated by the conflict, and their behaviour would have been affected accordingly. Nevertheless, SIRC did not find evidence that either the complainant's behaviour

in serving as counsel to her clients, or the CSIS officers' behaviour was unreasonable, threatening or intimidating.

As with all complaints, the complainant had the burden of proof. SIRC concluded that the complainant did not present sufficient evidence to prove the alleged intimidation and misconduct.

Nevertheless, SIRC concluded that the conflict between the two parties might have been avoided if CSIS policies permitted an individual not only to have counsel or another representative attend a security screening interview, but also to advocate for that individual during the interview process with CSIS.

SIRC recommended that the Service's policies be amended so that individuals are permitted to be accompanied and fully represented by counsel or another representative during a security screening interview conducted by CSIS.

Alleged abuse of human rights and unfair treatment

Report 2007-02

In this complaint filed with SIRC under Section 41 of the *CSIS Act*, the complainant alleged that CSIS had abused his human rights and those of his family, and that the Service had treated him unfairly. SIRC investigated the complaint and concluded that there was no evidence of any abuse of human rights as alleged. While SIRC did find that the complainant had been treated unfairly, it was to a much lesser degree than had been alleged by the complainant.

Allegations concerning CSIS's handling of evidence obtained by torture

Report 2007-03

SIRC reported a decision concerning a complaint pursuant to Section 41 of the *CSIS Act*, in which the complainant, Paul Copeland, alleged a "total lack of concern" by CSIS regarding evidence obtained by torture.

Noteworthy in this case is that immediately after SIRC began its investigation, the Government of Canada implemented a key recommendation made by Justice O'Connor in his report on the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. On December 12, 2006, the Honourable Frank Iacobucci

was appointed to undertake an inquiry into the actions of Canadian officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin. Therefore, SIRC decided that it would be inappropriate for the Committee to include any findings in its report that could be the subject of this inquiry.

In investigating Mr. Copeland's complaint, SIRC had access to classified information relevant to the allegations, including a classified version of the report of Justice O'Connor (hereafter referred to as the "Arar Report"). After having reviewed all the documentation made available, as well as the representations of the parties, SIRC did not find evidence of a "total lack of concern."

In its decision, SIRC noted that on June 29, 2005, CSIS had implemented two relevant recommendations contained in SIRC's review of the role of CSIS in the matter of Maher Arar.³ The first recommendation was to change CSIS operational policies so that it must consider the human rights record of a foreign state or agency when information received from those sources will be used in an application for targeting approval. The second recommendation was to amend a CSIS operational policy that governs the information included in a foreign-travel proposal so that it must consider the human rights records of foreign states or agencies regarding incoming visits or travel abroad.

Further, SIRC took into consideration Recommendation 14 made by Justice O'Connor in the Arar Report, which states:

"Information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture. Policies should include specific directions aimed at eliminating any possible Canadian complicity in torture, avoiding the risk of other human rights abuses and ensuring accountability."

SIRC views this recommendation as the standard that CSIS should apply when exchanging information. As Justice O'Connor further stated:

"Domestically, the Canadian Charter of Rights and Freedoms confirms the absolute rejection of the use of torture."

Although SIRC did not find evidence of a "total lack of concern" on the part of CSIS regarding evidence obtained by torture, it did find that at the time the complaint was made, CSIS lacked specific policies aimed at eliminating any possible Canadian com-

³ A complete list of SIRC reviews is available on SIRC's website (www.sirc-csars.gc.ca).

plicity in torture. As noted in the Arar Report, CSIS had no personnel with expertise in recognizing intelligence that may have been the product of torture, but “[r]ather, CSIS’s assessment focuse[d] on whether the Service can corroborate the information.”

SIRC found this lack of expertise hampered the Service in exercising due diligence, not only in assessing the reliability of information—particularly whether the information was obtained by torture—but also in assessing whether there was a credible risk that the exchange of information would cause or contribute to the use of torture.

SIRC noted the following advice provided by Justice O’Connor in his report:

“Canadian officials must be more sophisticated in their assessments, taking into consideration all of the available information in order to draw reasonable inferences about what may have happened. The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (Convention against Torture) provides that the human rights record of a country must be considered in assessing the risk of torture.”

During its investigation, SIRC was informed that CSIS has personnel with the expertise to assess the reliability of information. However, SIRC was neither informed nor could it determine whether CSIS has personnel with the expertise to make sophisticated assessments as to whether exchanges of information will create a risk of causing or contributing to any possible Canadian complicity in torture, or the risk of other human rights abuses.

In SIRC Review 2005-02 (CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post),⁴ SIRC had found a lack of any written documentation about possible human rights concerns cited by organizations such as Amnesty International and Human Rights Watch. The concerns related to the Service’s documentation of a separate and relatively new foreign arrangement with a particular intelligence agency. SIRC found that this lack of written documentation would not meet the standard of assessment as contemplated by Justice O’Connor in ensuring Canada’s non-complicity with human rights abuses.

With respect to arrangements with foreign states or agencies to collect and share information and intelligence, both Ministerial Direction and operational policy require that CSIS address a country’s human rights record. This includes any possible abuses by the security or intelligence organizations. Further, arrangements with

⁴ A complete list of SIRC reviews is available on SIRC’s website (www.sirc-csars.gc.ca).

countries that do not share Canada's respect for democratic or human rights will only be considered where contact is required to protect the security of Canada.

CSIS's policy requires that all applications for any targeting submission take into consideration the human rights record of any foreign state or agency whose information may be used to support the submission.

Based on these facts, SIRC found CSIS is concerned with human rights, but nevertheless may use information obtained by torture. Although it did not find a "total lack of concern" for evidence obtained by torture, SIRC did find that CSIS focused on the impact that torture might have on the reliability of information used in carrying out its responsibilities under the *CSIS Act*, rather than on its obligations domestically under the *Canadian Charter of Rights and Freedoms* and the *Criminal Code of Canada*, as well as internationally under the treaties signed by Canada that absolutely reject torture.

For purposes of this investigation, SIRC found that Justice O'Connor's findings and recommendations—as well as any future findings and recommendations by the Honourable Iacobucci's inquiry—will ensure that the use of information obtained through exchanges with foreign agencies is done in such a way that protects Canadians from threats to their security. These efforts will also respect the values of Canada's free and democratic society as reflected in the *Charter*, the *Criminal Code*, and its treaty obligations regarding the abhorrence of torture.

SIRC recommended that CSIS implement the recommendations directed at the Service in the Arar Report.

A second recommendation made as a result of this investigation cannot be disclosed for reasons of national security.

Alleged discriminatory practice

Report 2007-04

SIRC reported a decision on a complaint pursuant to Section 45 of the *Canadian Human Rights Act*. The complainant alleged that Transport Canada had discriminated against him on the grounds of race, national or ethnic origin, and religion by treating him in an adverse differential manner.

The Minister of Transport asked the Canadian Human Rights Commission to refer the case to SIRC.

The alleged discrimination concerned Transport Canada:

- not issuing the complainant an Airport Restricted Area Access Clearance Pass on grounds of religion and ethnic origin; and
- pursuing a policy and/or practice of denying security clearance to individuals of the complainant's ethnic origin.

Under Transport Canada's Airport Restricted Area Access Clearance Program (hereafter "the Program"), the complainant (who was working for a private-sector employer) needed site-access clearance to be issued a pass by the Airport Pass Control Office. This would have provided the individual with access to restricted areas within an airport. The aim of the Program is to prevent unlawful acts of interference with civil aviation. It does so by issuing a site-access pass to persons who meet the standards set out in this Program. The objective is to prevent uncontrolled entry into a restricted area of a listed airport by a person who falls within one of the listed categories of threats to security.

As part of the complainant's application process for a pass, the Director of Preventive Security for Transport Canada was provided with information about the complainant resulting from a criminal record check, a credit check and a CSIS indices check. The Director of Preventive Security decided to convene an Access Clearance Review Board, which took into consideration the national security concerns communicated by CSIS and the results of the criminal record check. The Review Board decided to recommend to the Minister of Transport the denial of the clearance. Subsequently the Minister denied the complainant site-access clearance. Since restricted-area access at the airport was a condition of employment, the individual's job was terminated.

The Minister of Transport made the decision without providing the complainant with the opportunity "to know the case against him" or to respond to the adverse information. Nor was the complainant provided any reasons for the denial. The Minister informed the individual that there was a 30-day deadline within which to seek from the Federal Court a judicial review of the decision.

SIRC found that:

1. The complaint of discrimination pertained to a practice that was based on considerations relating to national security, and hence was properly referred to SIRC pursuant to Subsection 45 (2) of the *Canadian Human Rights Act*.
2. The Minister's decision not to grant the site-access clearance, which resulted in the Airport Restricted Area Access Clearance Pass not being granted, was made in accordance with the relevant program, and was done for security considerations—not on prohibited grounds of discrimination based on the complainant's race, national or ethnic origin or his religion.
3. The security assessments conducted by CSIS and Transport Canada were flawed for two reasons:
 - a. the procedure relied on by the Review Board and the Minister of Transport under the Program was inherently unfair and breached the rules of natural justice, given the serious consequences of the Minister's decision—namely the loss of the complainant's employment; and
 - b. CSIS did not comply fully with its own procedures.

More specifically, SIRC found the procedure under the Program was inherently unfair and breached the rules of natural justice by:

- not providing the complainant with an opportunity to respond to any adverse information prior to the decision being taken by the Minister;
- not providing the complainant with reasons for the Minister's decision according to which the complainant could have made an informed choice to seek judicial review;
- relying on an inadequate security assessment; and
- failing to answer the complainant's counsel's telephone inquiries on a timely basis which, in all likelihood, would have had an impact on the complainant making an informed decision to seek judicial review within the 30-day deadline.

Given the serious consequences of the Minister's decision, which resulted in the loss of the complainant's employment, the complainant should have been afforded a fair process which adhered to the rules of natural justice.

SIRC recommended that the Canadian Human Rights Commission not investigate this complaint in accordance with Subsection 46 (2) of the *Canadian Human Rights Act*. It maintained that the Minister did not make his decision to deny the complainant site-access clearance based on a prohibited ground of discrimination, nor was Transport Canada pursuing a policy and/or practice of denying site-access clearance to individuals of the same ethnic origin as the complainant.

SIRC further recommended that the Minister provide the complainant with the opportunity to re-apply for the security clearance under the new policy.

Finally, SIRC recommended that if the complainant were to re-apply, CSIS or Transport Canada should conduct an interview with the complainant in the presence of counsel or any other representative. In addition, the complainant should be made aware of the right to record the interview, and that CSIS or Transport Canada also record the interview and retain a copy of the recording until the complainant has had an opportunity to exhaust any review process or until the retention period under the *Privacy Act* has expired, whichever is later.

Alleged improper advice to the Minister of Citizenship and Immigration

Report 2007-05

SIRC reported an investigation of a complaint made under Section 41 of the *CSIS Act* alleging that CSIS had provided improper advice to Citizenship and Immigration (CIC) in 2001 and 2004 regarding a complainant's application for permanent resident status in Canada under the former *Immigration Act*.

In this case, the complainant was a refugee from Pakistan. In his immigration documents, he had declared that while he was in Pakistan from 1985 until he immigrated to Canada in 1996, he had been a member of an organization called the Muttahida Quami Movement (otherwise referred to as "MQM"). In 2000, he was interviewed by CSIS, at which time he provided details of his past involvement with the MQM. He told the CSIS interviewer that he had not been involved with the MQM since arriving in Canada.

Following the interview, CSIS provided an inadmissibility brief to CIC in 2001. In 2004, CSIS updated their advice to CIC. At the time of the second inadmissibility brief, the *Immigration Act* had been replaced by the *Immigration and Refugee Protection Act (IRPA)*. Section 19 of the former Act had been replaced with Section 34 of the IRPA.

Much of SIRC's investigation focused on whether, by law, there are reasonable grounds to believe the MQM is an organization that is or was engaged in terrorism. The investigation also focused on whether the advice from CSIS to CIC regarding this issue was proper. SIRC received evidence from both the Service and the complainant on this issue. SIRC considered the wording of the *Immigration Act* as it was applied by CSIS in the 2001 inadmissibility brief that was later confirmed by

the 2004 inadmissibility brief and found that the advice from CSIS to CIC on this issue was proper.

However, SIRC found other aspects of the advice from CSIS to CIC were wrong or inaccurate and therefore improper. SIRC found no evidence to support a bona fide belief that the complainant has been a member of the MQM since arriving in Canada. This advice was wrong and was perpetuated by the second inadmissibility brief in 2004. SIRC also found an inaccurate statement in the 2001 inadmissibility brief.

Additionally, SIRC considered the exception set out in Section 19 (1)(f)(iii)(B) of the former *Immigration Act* whereby an applicant could not fall within the inadmissible class as set out in paragraph (f) or be deemed inadmissible, where the applicant has satisfied the Minister of Citizenship and Immigration that his or her admission would not be detrimental to the national interest. From a review of the CSIS analyst's assessment, the analyst did not address the exception.

Finally, the 2004 inadmissibility brief did not address the fact that the *Immigration Act* had been replaced by the *Immigration and Refugee Protection Act* and that the exception embedded in Section 19 (1)(f)(iii)(B) of the former *Immigration Act* is currently found in a general exception in Section 34 (2) in the *IRPA*. Therefore, it was improper for CSIS not to have updated their advice by referring to the new legislation. SIRC found that the advice in the 2004 inadmissibility brief was wrong because it did not take the new legislation into account.

SIRC also made two findings regarding procedure.

The first finding concerned the production of documents. On four occasions during the investigation, SIRC requested a copy of the relevant security screening guidelines or procedures relied on by CSIS for the provision of their advice to CIC. After the hearing, counsel for CSIS provided SIRC, pursuant to an undertaking, a copy of the Security Screening Procedures Guidelines which, to the best of the Service's knowledge, were in effect at the time the first inadmissibility brief was prepared. Security screening procedures for the purpose of preparing the second inadmissibility brief in 2004 were never formally approved. Although a witness for CSIS testified that all the procedures and guidelines were complied with in the preparation of the inadmissibility briefs, SIRC could not give much weight to that testimony since the witness had no personal involvement in the preparation of the briefs. Moreover, CSIS could not tell SIRC with full certainty what documents were relied upon in the preparation of the briefs.

The second finding concerned the destruction of the CSIS interviewer's notes. SIRC was informed that the interviewer had destroyed the notes taken during the interview with the complainant in accordance with CSIS operational policy, identified as OPS-217 *Operational Notes* and thus the notes were not available to SIRC for purposes of the investigation. SIRC determined that the destruction of the notes did not hinder its investigation. However, SIRC found that the notes of a subject interview for immigration screening may be required as evidence or information for investigations or proceedings before the courts or administrative tribunals and therefore should be retained by the Service. SIRC has recommended on other occasions that notes of interviews not be destroyed.

Finally, SIRC recommended that CSIS prepare fresh advice to CIC, to satisfy the Minister of CIC that the presence of the complainant in Canada would not be detrimental to the national interest in accordance with Subsection 34(2) of the *IRPA*, or if required, could be used by the complainant to seek what is referred to as "Ministerial Relief" in respect of Subsection 34(2) under the *IRPA*.

Alleged unreasonable delay in processing a site-access clearance

Report 2007-06

SIRC reported on a complaint made pursuant to Section 41 of the *CSIS Act*, regarding the delay by CSIS in completing its security assessment for the purposes of the complainant's employment. The complainant had received an offer of employment that was conditional upon the complainant successfully obtaining a reliability and site-access clearance. The employer specified in the letter of offer the date by which the complainant was to obtain the reliability and site-access clearance, failing which the employer would have the option of either extending the time for the satisfaction of the condition of employment or of rescinding the offer. When SIRC began the hearing of this complaint, CSIS had not completed its security assessment. More than twenty months had elapsed since the complainant had received the offer of employment, and the complainant had been subjected to three subject interviews by CSIS.

SIRC concluded that when the complainant first wrote the Director of CSIS (approximately two months after the complainant had received the letter of offer) to complain about the time taken by CSIS to complete its security assessment, the complaint was premature, notwithstanding the date specified by the employer in the offer of employment. SIRC also found that although there was an accumulation of moderate delays, the overall time taken by CSIS to complete its security assessment

during the first seven months was reasonable. However, SIRC found that after the first seven months, although the delays were not deliberate, the time taken by CSIS to conduct its security enquiries was not reasonable and the delays could have been avoided.

SIRC made four recommendations:

- that CSIS take all necessary steps to ensure the adoption of its *Security Screening Procedures Manual* and *Security Screening Investigator's Guidebook* before June 30, 2008;
- that CSIS adopt guidelines to ensure that the information recorded and contained in the security screening database accurately reflect the status of the file to enable all users of the system to be as fully aware as possible of the file without having to review the hard-copy file and that appropriate diary dates be included in its security screening database;
- that CSIS policy be revised as expeditiously as possible to prevent the destruction of recorded or written notes which may be required as evidence in proceedings before the courts or administrative tribunals; and
- that CSIS provide its advice forthwith with regard to the complainant's security assessment.

Section 2

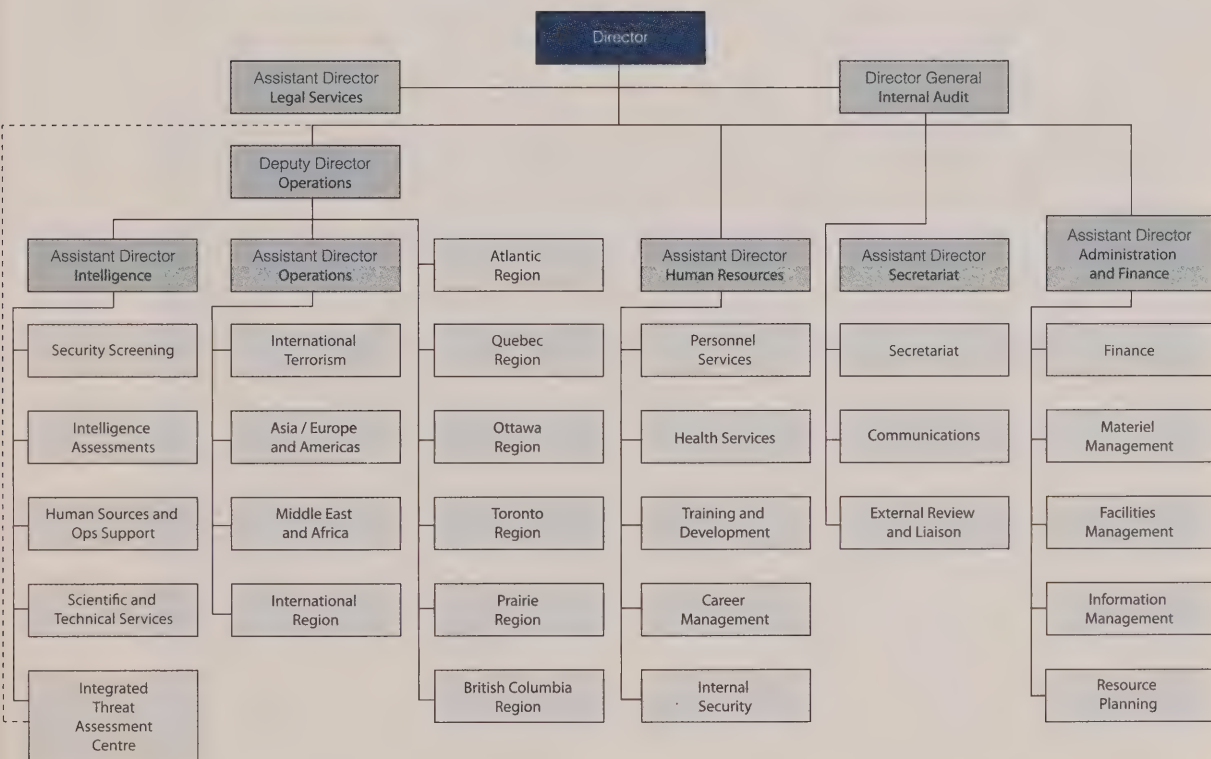
CSIS operational activities and accountability mechanisms

A. CSIS operational activities

The Deputy Director Operations, who reports to CSIS's Director, is responsible for three groups:

- **Intelligence**, consisting of five branches (Security Screening, Intelligence Assessments, Human Sources and Operations Support, Scientific and Technical Services, and the Integrated Threat Assessment Centre);
- **Operations**, consisting of three branches and one region (International Terrorism, Middle East and Africa, Asia, Europe and Americas, and International Region); and
- **Six regions**.

Canadian Security Intelligence Service



i. Intelligence

SECURITY SCREENING BRANCH

As a key component of Canada's national security framework, security screening provides one of the Service's most visible functions.

The Security Screening Branch has two program streams: government screening and immigration screening. In response to an increasing number of screening requests over the past several years, the branch has attempted to improve its technical and case management functions to ensure that they continue to provide timely, relevant and accurate assessments that meet client expectations. The branch has also consulted with government clients to guide them through new rules concerning the security screening process.

Government screening provides security assessments—an appraisal of an individual's loyalty to Canada and, so far as it relates thereto, the reliability of the individual—for all government departments and institutions, except the Royal Canadian

CSIS advice on security screening can take one of five forms:

1. **Notices of assessment** (NOA) are issued in those government- and immigration screening cases when CSIS finds no adverse information on an applicant.
2. **Incidental letters** are issued to Citizenship and Immigration Canada (CIC) and to the Canada Border Services Agency (CBSA) when the Service has information about an applicant who is or has been involved in non-security related activities described under the *Immigration and Refugee Protection Act (IRPA)*.
3. **Information briefs** are issued in government screening cases when CSIS has information that could have an impact on the requesting agency's decision to grant an applicant a security clearance or site access. It is also provided in immigration screening cases when the Service has information that an applicant is or was involved in activities that do not necessarily warrant inadmissibility for entry into Canada.
4. **Inadmissibility briefs** are issued to CIC/CBSA when an applicant is deemed to be inadmissible to Canada under the security provisions of the *IRPA*.
5. **Denial briefs** are issued when the Service recommends to a requesting agency that a security clearance or site access be denied to an individual.

Mounted Police (RCMP), for which CSIS performs indices and Out-of-Country (OCC) checks, including joint subject interviews for cause. It is also involved in a site-access program for airports, port and marine facilities, the parliamentary precinct and nuclear power facilities, as well as providing assessments to provincial departments. These programs are meant to enhance security and reduce the potential threat from terrorist groups and foreign governments that seek to gain advantage by obtaining authorized access to classified information or other assets, materials and sensitive sites.

Traditionally, the largest clients of this service have been Public Works and Government Services Canada and the Department of National Defence (DND), accounting for over 30 percent and 16 percent respectively of all requests in 2007–08.

As indicated in Table 2, in 2007–08, CSIS received 50,300 requests for new or updated security clearances and provided 48,800 security assessments to federal departments. The volume of requests was down slightly from the previous fiscal year, as was the number of security assessments. The biggest change was a decrease in the number of requests from DND.

Table 2
CSIS government security screening*

	2005-06	2006-07	2007-08
Requests from DND	9,200	13,100	8,800
Requests from other departments or agencies	32,900	38,100	41,500
Total	42,100	51,200	50,300
Assessments issued to DND	8,900	13,100	8,300
Assessments issued to other departments or agencies†	28,900	41,800	40,500
Total	37,800	55,000	48,800

* Figures have been rounded to the nearest 100.

† This number includes assessments performed for provincial governments and for access to nuclear facilities.

As part of its efforts to track efficiency in responding to security screening requests, CSIS calculates its turnaround times using a median number of calendar days. As indicated in Table 3, the median turnaround times decreased compared to the previous year's levels, the exception being an increase for Level III (Top Secret) assessments.

However, the median times for this category were calculated differently in 2007–08, which resulted in a rise in the median time in comparison to previous years. For 2007–08, median times for Level III clearances exclude updates for those who already have this clearance, a process that takes considerably less time than requests for new or upgrade assessments.⁵ For example, while the median turnaround time for new and upgrade Level III assessments for DND is 164 days, the median time for updates is 29 days. Similarly, for non-DND clients the median turnaround time is 186 days for new or upgrade Level III assessments, compared to four days for updates.

Table 3
Median turnaround time (in calendar days)

		2005–06	2006–07	2007–08
DND	Level I (Confidential)	24	40	23
	Level II (Secret)	19	40	28
	Level III (Top Secret)	39	82	164 (new) 29 (updates)
Non-DND	Level I (Confidential)	15	32	17
	Level II (Secret)	13	21	13
	Level III (Top Secret)	60	47	186 (new) 4 (updates)

The Service does not decide who receives a security clearance. Rather, it advises the requesting department or agency of information that could have an impact on their decision to grant a clearance. On rare occasions, CSIS will indicate to a requesting agency that the Government Security Policy threshold for denying clearance has been met. However, it is the responsibility of the requesting agency to grant, revoke or deny a clearance. In 2007–08, the Service issued eight information briefs reporting information of an adverse nature. Two denial briefs were issued.

⁵ Individuals with a Level III (Top Secret) clearance must renew/update their clearance level every five years. New and upgrade assessments include those who are applying for a clearance and those who are applying for a higher-level clearance (e.g., someone with a Level I clearance who applies for a Level III clearance).

CSIS also provides site-access screening (see Table 4). Unlike a government security clearance, a site-access clearance only gives an individual access to certain secure areas or provides accreditation for special events. In 2007–08, CSIS received over 67,500 requests for this type of screening and provided no information briefs to requesting agencies. The increase in requests for access to nuclear facilities in 2006–07 was a result of a five-year renewal cycle for pre-existing clearances. The number of these requests therefore dropped in 2007–08. There was also a decrease in the number of requests associated with the Free and Secure Trade (FAST) program.

The Service provided over 1,300 assessments for special events in 2007–08.

Table 4
Site-access screening*

	2005–06	2006–07	2007–08
Parliamentary precinct	1,000	1,100	1,100
Airport restricted-access area	37,600	39,300	36,800
Nuclear facilities	10,600	17,900	9,200
Free and Secure Trade (FAST)	3,100	23,100	10,700
Special events accreditation	5,600	0	1,300
Marine Transportation Security Clearance Program†	N/A	N/A	6,300
Other government departments	2,400	2,500	2,100
Total	60,300	83,900	67,500

* Figures have been rounded to the nearest 100.

† The Marine Transportation Security Clearance Program, which provides security assessments in relation to the security of Canada's ports, became operational in December 2007.

Immigration screening helps to ensure that individuals who pose a threat to security and/or are inadmissible under the *IRPA* do not gain entry or obtain status in Canada. This program provides security advice to:

- a) identify whether or not citizenship applicants will engage in activities that constitute a threat to the security of Canada;
- b) identify individuals who are inadmissible on security grounds under Section 34(1) of the *IRPA*;
- c) identify visitor and refugee claimants at Canadian ports of entry who are inadmissible for security reasons; and
- d) screen those requesting visitor visas from countries that pose a terrorist, espionage and transnational criminal activity threat.

In 2007–08, the branch received 94,400 requests under various immigration screening programs (see Table 5). The number of requests received within and from outside Canada was similar to the previous year, while the number of refugee determination requests decreased. The number of front-end screening requests increased from the previous year.

Table 5
Immigration security screening

	Requests*			Briefs		
	2005–06	2006–07	2007–08	2005–06	2006–07	2007–08
Within and outside Canada†	63,200	62,800	66,000	133	201	195
Front-end Screening††	17,100	17,900	21,800	89	143	117
Refugee determination†††	11,700	11,600	6,600	127	153	142
Subtotal	92,000	92,300	94,400	349	497	454
Citizenship applications	308,000	227,300	190,000	120	155	109
Total	400,000	319,600	284,400	469	652	563

* Figures have been rounded to the nearest 100.

† This includes permanent residents from within and outside Canada (excluding the Refugee Determination Program), permanent residents from within the United States and applicants from overseas.

†† Individuals claiming refugee status in Canada or at ports of entry.

††† Refugees, as defined by the *IRPA*, who apply from within Canada for permanent resident status.

CSIS finds no adverse information in the majority of its screening investigations of refugee claimants or immigration/citizenship candidates. In 2007–08, the Service issued 325 information briefs, 129 inadmissibility briefs and one incidental letter related to immigration cases.

In recent years, the Service's turnaround times for providing information or inadmissibility briefs were generally quite lengthy. In 2007–08, information briefs related to immigration cases took a median of 508 calendar days for an application filed in Canada, 620 days for those filed from the United States and 150 days for those filed abroad. Information briefs related to permanent resident applicants who are refugees in Canada had a median turnaround time of 497 days, and those for files subject to the Front-End Screening Program had a turnaround time of 339 days.

Table 6 provides a three-year highlight of the Service's median turnaround time for providing notices of assessments.

Table 6
Turnaround time (in days) for notices of assessment

	2005–06	2006–07	2007–08
Citizenship	1	1	1
Immigration (Canada)*	70	78	59
Immigration (USA)**	62	29	45
Overseas immigration	16	14	20
Refugee determination	96	98	64
Front-end screening	23	19	28

* This includes certain classes of individuals who apply for permanent resident status within Canada.

** This includes persons who have been legally admitted to Canada for at least one year, and who may submit their application to Citizenship and Immigration offices in the United States.

Other screening activities

In 2007–08, the Security Screening Branch also vetted 111,300 visa applications for foreign programs. In addition, the branch was involved in the following two programs:

- **The Trusted Traveller Program** — a pre-clearance program for individuals who travel frequently to the United States. This program is currently under development; and
- **Passenger Protect** — the branch worked with other government departments in developing airline passenger screening programs, in particular the domestic “no-fly” program, which became operational on June 18, 2007.

INTELLIGENCE ASSESSMENTS BRANCH

The Intelligence Assessments Branch consolidates the key analytical function of the Service and centralizes its main intelligence reporting mechanisms. It develops strategic and operational analyses of current threats and emerging issues, and produces *Intelligence Assessments*, *Threat and Risk Assessments* and *Perspectives*.

In recent years, the branch has undergone a series of changes in an attempt to respond to the growing demand within the Service and across government for strategic and operational assessments. As part of this process, the branch has engaged in dialogue with federal partners and clients to ensure that CSIS continues to provide relevant and timely assessments that meet the needs of clients. The branch has sought opportunities to coordinate with partners within the assessment community to identify common areas of interest and produce community assessments. Likewise, it has created internal mechanisms to promote an ongoing dialogue with collectors within the Service to ensure that analytical support is provided in a timely fashion to assist in investigations.

This branch also has a role in the Terrorist Entity Listing process both in regards to listing new entities and renewing those already listed. The Service prepares Security Intelligence Reports (SIRs) on groups that are believed to be, or act on behalf of, a terrorist entity. This report outlines the Service’s findings and forms the basis for consideration by the Governor-in-Council on whether to approve that a group be listed under Section 83.05 of the *Criminal Code of Canada*. Every two years, the Minister of Public Safety is obliged, under the *Criminal Code*, to review the Terrorist Entity Listing to determine whether there are still reasonable grounds for an entity to be listed and make a recommendation to the Governor-in-Council accordingly.

The Minister's most recent review of the listing commenced in February 2008 and is to be completed this fall.

HUMAN SOURCES AND OPERATIONS SUPPORT BRANCH

This branch provides a range of support and coordination services including risk management and analytical expertise for operational activities across the Service. It is the policy centre in a number of areas including operational security, multilingual services and management of human sources. It also contains the Threat Management Centre, which provides 24/7 support to operational staff at headquarters and regional and Foreign Offices, and it provides support to the Service's involvement in major special events such as last year's North American Leaders' Summit and the upcoming 2010 Olympic Games in Vancouver.

SCIENTIFIC AND TECHNICAL SERVICES BRANCH

This branch develops and deploys technical tools and mechanisms to support the operations and investigations of CSIS's other branches.

INTEGRATED THREAT ASSESSMENT CENTRE

The Integrated Threat Assessment Centre (ITAC) produces assessments that warn the government about terrorist threats to Canada and to Canadian interests abroad. Once completed, ITAC's threat assessments are distributed to domestic and foreign partners. Additionally, ITAC acts as a distribution hub for threat assessments produced by counterparts in the United States, the United Kingdom, Australia and New Zealand.

During the period under review, ITAC issued 348 threat assessments and redistributed over 1,300 others produced by allied fusion centres. ITAC also published *Media Watch* each business day for distribution to clients. Further, ITAC provided over 120 briefings to its domestic clients, including the Petroleum Industry Annual Safety Seminar, the Canadian Association of Chiefs of Police Liaison Conference, the Cyber Security Task Force and a critical infrastructure conference in the United States.

During the period under review, ITAC assumed responsibility for the Threat Assessment Unit, which provides time-sensitive evaluations of potential threats to Canadians and Canadian interests in Canada or abroad, or to foreign interests or nationals in Canada. ITAC provided assessments of key issues for the Government of Canada and in relation to the North America Leaders' Summit at Montebello, Quebec in August 2007. Also of note, ITAC produced three papers in collaboration with the Canadian Centre of Intelligence and Security Studies at Carleton University.

ITAC continued its planning work regarding a 24/7 centre with an integrated analytical capacity.

ii. Operations

Under Operations, four branches are responsible for investigating all threats emanating from within their respective geographic areas, with the exception of the International Terrorism Branch, which focuses exclusively on al Qaida and al Qaida-inspired groups regardless of geographic boundaries.

Middle East and Africa Branch

This branch concentrates its investigative effort on threats that emanate from, or have as their major focus in, countries in the Middle East and Africa. This includes issues of terrorism, foreign-influenced activities, the proliferation of weapons of mass destruction and espionage.

Asia, Europe and Americas Branch

This branch investigates threats emanating from its vast area of geographic responsibility, namely espionage, terrorism (including domestic extremism) transnational criminal activity and foreign-influenced activities.

International Terrorism Branch

This branch conducts investigations globally and within Canada, focusing on Islamist extremists engaged in a variety of terrorist-related activities that pose a direct threat to Canadians and Canadian interests. Notable among this branch's areas of interest is the radicalization of Islamists within Canada.

International Region

This branch manages the Service's liaison with foreign agencies and coordinates visits to CSIS headquarters and CSIS regional offices by foreign representatives. It is also responsible for coordinating all Section 17(1) arrangements with intelligence or enforcement agencies, as well as the operation of the Service's Foreign Offices abroad. The Service relies on these offices to assist in liaising with foreign security and intelligence agencies, as well as to coordinate visits to CSIS headquarters and regional offices by foreign representatives.

FEDERAL COURT WARRANTS AND WARRANT STATISTICS

Warrants are one of the most powerful and intrusive tools available to the Service. They provide CSIS with Federal Court authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telephone communications. For this reason, the use of warrants by CSIS is an important aspect of SIRC's reviews.

Each year, SIRC collects statistics on the Service's warrant applications and on warrants granted by the Federal Court under Sections 12 and 16 of the *CSIS Act*. SIRC does not examine all aspects of warrants granted to the Service, particularly since this is part of the vital accountability function provided by the Federal Court. However, as part of its review activities, SIRC does consider whether the Service adheres to the warrant approved by the Federal Court (i.e., how the warrant powers were used by CSIS).

In 2007–08, the Federal Court approved 71 new warrants—a notable increase from the previous year. The Federal Court also approved the replacement or renewal of 182 warrants, which is also an increase from the previous year's levels. During the same period, 56 warrants were either terminated or expired without being renewed. No warrant applications were denied by the Federal Court. In one instance, the Federal Court denied the Service's request for a foreign telecommunications warrant authorizing the interception, outside Canada, of the communications of subjects under investigation. In its decision, the court ruled that it had no jurisdiction to issue the warrant sought under the *CSIS Act*.

Table 7
Warrant statistics

	2004–05	2005–06	2006–07	2007–08
New warrants	40	24	42	71
Replaced or renewed	207	203	134	182
Total	247	227	176[†]	253^{††}

[†] Included in this number were 25 urgent warrants.

^{††} Included in this number were 19 urgent warrants.

B. Reporting requirements

CSIS DIRECTOR'S ANNUAL REPORT (2006–07)

Every year, the Director of CSIS submits a classified report to the Minister of Public Safety. It describes in detail the priorities and operational activities of the Service. The Inspector General of CSIS examines this report and submits to the Minister a certificate that attests the extent to which she or he is satisfied with its contents. Next, the Minister sends a copy of both documents to SIRC for its review, as required by Section 38(a) of the *CSIS Act*.

In the 2006–07 edition of the report—the first one to be issued following the realignment of operational resources within CSIS—the Director noted that the realignment provides the Service with a flexible organizational structure that can be easily modified to future operational needs.

In addition to summarizing the Service's use of human sources during the year, the report identified the activities of each operational branch and specialized group within CSIS, as well as all domestic and foreign arrangements, as provided under Section 17 of the *CSIS Act*.

The Director reported that CSIS had suspended its relationships with five human sources because of criminal activity. He further noted that CSIS had not directed the sources to undertake this activity and that the Service immediately took corrective measures upon learning about the incidents. The Director highlighted CSIS's role in identifying suspected Russian spy Paul William Hampel, and of the Service's role in expelling this individual from Canada. The Director also reported that the Service's Middle East and Africa Branch terminated an investigation because of a lack of reporting of threat-related activities.

Of particular note, the Director drew the Minister of Public Safety's attention to the challenges that CSIS faces with the rapid growth and changes to Internet-related technologies. He indicated that a remedy for these challenges would be for Parliament to pass legislation, such as the *Technical Assistance to Law Enforcement Agencies Act*. The legislation was tabled in November 2005 but was not passed because of the federal election that was called immediately afterwards.

Readers should note that CSIS posts public, unclassified reports on its website (www.csis-scrs.gc.ca).

CERTIFICATE OF THE INSPECTOR GENERAL OF CSIS (2006–07)

Established in 1984 under the *CSIS Act*, the Inspector General of CSIS functions as the “eyes and ears” of the Minister of Public Safety, reviewing the Service’s operations and providing assurance that CSIS is complying with Ministerial Direction, operational policy and the *CSIS Act*.

Every year, the Inspector General submits a certificate to the Minister stating the extent to which he or she is satisfied with the CSIS Director’s Annual Report. This certificate informs the Minister of any unreasonable or unnecessary exercise of CSIS powers, as well as any instances of the Service failing to comply with either the *CSIS Act* or Ministerial Direction.

In the latest certificate, the Inspector General was satisfied with the CSIS Director’s 2006–07 Annual Report, stating that the Service has not acted beyond the framework of its statutory authority, had not contravened any Ministerial Directions, and had not exercised its powers unreasonably or unnecessarily.

However, the Inspector General expressed concern that there had been an increasing number of instances of non-compliance with CSIS operational policy, as well as a greater number of transcription errors in documents. Most of the instances of non-compliance were administrative errors. She also remarked on the length of time required to develop or update operational policies in response to changing requirements and activities.

For more information about the Certificate of the Inspector General (CSIS), please refer to the Public Safety website (www.publicsafety.gc.ca).

UNLAWFUL CONDUCT BY CSIS

Under Section 20(2) of the *CSIS Act*, the Director of CSIS must submit a report to the Minister when, in the Director’s opinion, a CSIS employee may have acted unlawfully in performing his or her duties or functions. The Minister, in turn, must send the report with his or her comments to the Attorney General of Canada and to SIRC. In 2007–08, no CSIS employee acted unlawfully, and no such reports were issued.

DISCLOSURE OF INFORMATION

Section 19 of the *CSIS Act* prohibits the disclosure of information obtained by the Service in the course of its investigations except in the following specific circumstances:

1. Information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law may be disclosed to a law enforcement agency having jurisdiction over the matter, or to the Minister of Public Safety or the Attorney General of the province in question;
2. Information related to the conduct of Canada's external relations may be disclosed to the Minister of Foreign Affairs;
3. Information related to the defence of Canada may be disclosed to the Minister of National Defence; and
4. Information that, in the opinion of the Minister, is essential to the public interest, may be disclosed to any Minister of the Crown or employee of the Public Service of Canada.

Of note, Section 19(2)(d) gives the Minister of Public Safety the power to override any invasion-of-privacy concerns, authorizing the Service to disclose information deemed to be in the national or public interest. When such information is released, the Director of CSIS must submit a report to SIRC. This is an exceedingly rare occurrence—there have been only two disclosures under this section of the *Act*.

The Service may also disclose information verbally or in writing to any law enforcement body or federal government entity, such as the Department of National Defence and Foreign Affairs and International Trade Canada. When CSIS permits the use of its information by the RCMP in judicial proceedings, it must do so in writing.

The Service provided over 90 disclosure letters during fiscal year 2007–08.

C. Foreign and domestic arrangements

Sections 13 and 17 of the *CSIS Act* allow CSIS to enter into arrangements with foreign and domestic organizations or agencies in order to perform its duties and functions. SIRC receives copies of these arrangements as they are initiated, and examines a selection of them every year.

ARRANGEMENTS WITH DOMESTIC AGENCIES

CSIS often collaborates with federal departments and agencies, provincial governments and law enforcement agencies. Since 9/11, more groups have been involved in national security, including police forces and other government partners. This creates a challenge for the Service, as it must cultivate and maintain healthy relationships with both new and existing partners to ensure that information is exchanged efficiently and that joint operations are conducted effectively.

Although many domestic arrangements take the form of a Memorandum of Understanding (MOU), CSIS may collaborate with any domestic agency whether or not an MOU is in place.

As of March 31, 2008, CSIS had 39 MOUs with domestic partners: 29 with federal departments or agencies and 10 with provincial and municipal entities.

In 2007–08, SIRC examined the Service's arrangement with Transport Canada, focusing on the Service's contribution of security screening information in support of two of that department's programs: the Marine Transportation Security Clearance Program and the Passenger Protect Program. Transport Canada is responsible for ensuring that Canadian aviation, marine, railway and road transportation systems are safe, efficient and accessible.

With respect to the Marine Transportation Security Clearance Program, SIRC found that, although this program is not yet fully operational, CSIS has worked collaboratively with Transport Canada to reduce the risk of security threats by conducting background checks on marine workers who have access to certain areas or perform certain duties. In terms of the Passenger Protect Program, SIRC found that CSIS has worked effectively with Transport Canada (along with the RCMP, which also contributes to the program) to ensure that individuals placed on the so-called "no-fly list" do pose a demonstrable threat to aviation security, and that decisions to place individuals on this list are based on clearly defined criteria.

More information about these programs can be found on Transport Canada's website (www.tc.gc.ca).

ARRANGEMENTS WITH FOREIGN AGENCIES

As of March 31, 2008, CSIS had 276 arrangements with agencies in 147 countries. New foreign arrangements require the approval of the Minister of Public Safety, in consultation with the Minister of Foreign Affairs. Even without such an arrangement, CSIS can still accept unsolicited information from an agency or organization of a foreign country. The Minister approved five new arrangements in 2007–08 and expanded three existing ones.

In 2007–08, SIRC examined foreign arrangements that had been restricted by the Service because of concerns relating to a country's or agency's human rights record, reliability, or ability to protect information provided by the Service. In general, restricted arrangements prevent CSIS from sharing operational information with an agency, although this does not prevent the Service from receiving unsolicited information concerning Canada's safety and security from a restricted agency.

SIRC found that CSIS adhered to its self-imposed restrictions with the agencies in question. SIRC also found that the Service performed well in terms of balancing the need to collect vital security intelligence information, while remaining aware of the potential problems of dealing with a restricted agency.

D. Policy and governance

NATIONAL REQUIREMENTS FOR SECURITY INTELLIGENCE

The Minister of Public Safety issues National Requirements for Security Intelligence, which contain general direction from government regarding where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis and advisory responsibilities.

The 2006–08 National Requirements directed CSIS to continue to maintain a flexible capability to meet Canada's evolving security intelligence needs by relying on risk management. The Minister noted that today's threat environment is increasingly international and transnational in nature, with many offshore threats to Canada's security requiring foreign investigations. CSIS was therefore directed to continue to investigate threats to Canada's security both within Canada and abroad.

For 2006–08, the Minister directed CSIS to pursue the following security intelligence priorities:

- Safeguarding against—and advising the government of—the possibility of a terrorist attack occurring in or originating from Canada, or affecting Canadian citizens or assets abroad;
- Continuing to conduct research and analysis in support of the listing of terrorist entities under the *Criminal Code of Canada* and combating terrorist financing;
- Supporting the Government of Canada's efforts in Afghanistan;
- Working closely with other government departments to combat transnational criminal activity;
- Investigating threats to Canada's national security arising from activities of countries that engage in espionage;
- Continuing to identify and investigate countries and groups that have or may attempt to acquire weapons of mass destruction, and advising the government of the threats posed by these activities;
- Supporting the collection of foreign intelligence in Canada to assist the Minister of Foreign Affairs and/or the Minister of National Defence pursuant to Section 16 of the *CSIS Act*;
- Delivering security screening programs to federal departments, agencies and other clients;

- Providing the Government of Canada with intelligence assessments and ensuring that CSIS keeps itself informed of political, social and economic environments from which threats to the security of Canada may emerge; and
- Ensuring CSIS's technical equipment and information systems meet the requirements of its investigations.

MINISTERIAL DIRECTION

Under Section 6(2) of the *CSIS Act*, the Minister of Public Safety may issue written directions governing CSIS's activities and investigations. The last time the Minister issued such direction was in 2001; when a compendium was provided to SIRC. In July 2008, however, SIRC received the latest Ministerial Direction for 2008–2009.

CSIS OPERATIONAL POLICY

CSIS administrative, security, human resources and operational policies embody rules and procedures that govern the range of activities undertaken by the Service. Administrative, security and human resources policies are all internal corporate policies. Operational policies, which describe how CSIS employees should perform their duties, are updated regularly in accordance with government policy, legislative and other changes.

In 2007–08, CSIS revised and/or published over 140 policies. Also, more than 70 additional policies were initiated or under development during the same period. Many revisions were administrative in nature. The remainder were operational and pertained to, among others things, targeting levels and approvals process, as well as security screening and warrant powers. In addition, as part of a project launched by the Director in 2006–07, the Service continued its efforts to review all operational policies to determine where executive and management responsibilities must be delegated.

GOVERNOR-IN-COUNCIL REGULATIONS AND APPOINTMENTS

Section 8(4) of the *CSIS Act* states that the Governor-in-Council may issue regulations to the Service concerning the powers and duties of the Director of CSIS, as well as the conduct and discipline of Service employees.

The Governor-in-Council did not issue any regulations in 2007–08.

Section 3

About SIRC

About SIRC

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Gary Filmon, P.C., O.M., who was appointed on June 24, 2005. The other Members are the Honourable Raymond Speaker, P.C., O.C., and the Honourable Roy Romanow, P.C., O.C., Q.C.

The term of the Honourable Baljit S. Chadha, P.C. ended on February 20, 2008. On April 22, 2008, the Honourable Aldéa Landry, P.C., C.M., Q.C. tendered her resignation from SIRC.

All Members of SIRC are Privy Councillors who are appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties.

In addition to attending monthly committee meetings, members preside over complaints hearings, prepare reviews and complaint reports in consultation with SIRC staff, visit CSIS regional offices, address parliamentary committees and exercise other duties associated with their responsibilities.

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 20, located in Ottawa. The staff comprises a Senior Counsel, a Senior Advisor, a Corporate Services Manager, Counsel, a Senior Paralegal (who also serves as Access to Information and Privacy Officer/Analyst), plus researchers and administrative staff.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

Committee activities

May 23–25, 2007: The Honourable Roy Romanow and Senior Counsel were speakers at a symposium marking the 25th anniversary of the *Canadian Charter of Rights and Freedoms* entitled “A Living Tree: The Legacy of 1982 in Canada’s Political Evolution,” hosted by the Saskatchewan Institute of Public Policy.

June 7–8, 2007: The Chair, the Executive Director and a Member of SIRC attended the International Intelligence Review Agencies symposium on accountability of intelligence and security agencies and human rights. The Chair delivered a speech to participants at this event, which was hosted by the Review Committee on the Intelligence and Security Services and the Faculty of Law at Radboud University (Netherlands).

June 10–12, 2007: The Chair, Members, the Executive Director and selected staff attended the International Conference on the Administration of Justice and National Security in Democracies, hosted in Ottawa by the Federal Court of Canada.

June 14, 2007: The Executive Director and senior staff met with the Australian Inspector General.

June 18, 2007: The Executive Director, accompanied by senior staff, appeared before the Senate Standing Committee to describe SIRC’s role and powers as a review body and quasi-judicial complaints tribunal.

Continued on page 56

Committee activities

(continued)

September 20–21, 2007: The Executive Director attended a conference in Ottawa, entitled "Protecting Security and Human Rights: The Case of Migration in Canada," hosted by the Institute for Research on Public Policy.

November 13, 2007 and March 31, 2008: At Carleton University, the Executive Director lectured on SIRC's role and mandate to students of a course on National Security and Intelligence in the Modern State.

November 28, 2007: The Executive Director and senior staff met with officials from the Norwegian Parliamentary Intelligence Oversight Committee.

November 30–December 2, 2007: The Executive Director was a panellist at a conference hosted by the Justice Institute of British Columbia's Committee on Diversity and Policing. The conference was entitled "Balance between Security, Human Rights and Accountability."

January 23, 2008: The Senior Counsel was a guest lecturer on National Security Law at the Faculty of Law, University of Ottawa.

As part of their ongoing work, the Chair of SIRC, Committee Members and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of the security intelligence community.

These exchanges are supplemented by discussions with academics, security and intelligence experts and other relevant organizations. These activities enrich SIRC's knowledge about issues and opinions affecting national security intelligence.

SIRC staff also visits CSIS regional offices on a rotating basis to examine how Ministerial Direction and CSIS policy affect the day-to-day work of investigators in the field. These visits give Committee Members an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. It is also an opportunity to communicate SIRC's focus and concerns.

During the 2007–08 fiscal year, SIRC staff visited two regional offices.

BUDGET AND EXPENDITURES

SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures. Table 8 below presents a breakdown of estimated and actual expenditures.

Table 8
SIRC expenditures 2007–08

	Estimates	Actual
Personnel	\$1,900,000	\$1,844,000
Goods and Services	\$1,000,000	\$781,000
Total	\$2,900,000	\$2,626,000

INQUIRIES UNDER THE *ACCESS TO INFORMATION ACT* AND *PRIVACY ACT*

The public may make requests to SIRC under both the *Access to Information Act* and the *Privacy Act*. Table 9 outlines the number of requests SIRC has received under these acts for the past three fiscal years.

Table 9
Requests for release of information

	2005–06	2006–07	2007–08
<i>Access to Information Act</i>	17	12	15
<i>Privacy Act</i>	5	2	2

Recommendations

Summary of SIRC recommendations concerning reviews

	SIRC recommended that...
Review 2007-01	<ul style="list-style-type: none"> • CSIS employees submit a standard, written record of non-operational information exchanged with foreign partners. This would be placed in both the relevant "cooperation with" file and operational database. The written record of non-operational information exchanged should also cross-reference the operational information exchanged with those foreign partners. • When CSIS is cooperating with a foreign agency, the Service should establish a separate Section 17 foreign arrangement with that agency to conform with the <i>CSIS Act</i>, Ministerial Direction and operational policy.
Review 2007-02	<ul style="list-style-type: none"> • CSIS consult with the Treasury Board Secretariat to clarify its responsibility to investigate incidents reported under the Government Security Policy, and to explore the value of enhancing interdepartmental liaison in order to advise departments of their security screening responsibilities under the policy.
Review 2007-04	<ul style="list-style-type: none"> • CSIS review the criteria used to conduct risk assessments, and that the Service define more precisely the high-risk situations for which it is necessary to consult with the Minister of Public Safety.
Review 2007-05	<ul style="list-style-type: none"> • CSIS should reconsider its policy structure to accommodate its increasing activities outside Canada. • CSIS standardize its risk assessments with detailed and consistent terminology that is reflected in operational policy.

	SIRC recommended that...
Review 2007-06	<ul style="list-style-type: none">• Debates about whether a targeted group is in fact a terrorist organization should be included in future targeting discussions by CSIS.
Review 2006-08* <small>* Note: This review was not finalized until after the 2006-07 annual report went to print.</small>	<ul style="list-style-type: none">• With respect to the Service's investigation of certain individuals believed to be second-generation terrorists, or recent converts to extremist interpretations of Islam, CSIS should clearly define this issue-based investigation when it is next renewed and determine whether it should focus on issues of increasing concern.

Summary of SIRC recommendations concerning complaints

	SIRC recommended that...
Report 2007-01	<ul style="list-style-type: none"> • CSIS policies be amended so that individuals are permitted to be accompanied and fully represented by counsel or another representative during a security screening interview conducted by the Service.
Review 2007-03	<ul style="list-style-type: none"> • CSIS implement the recommendations directed at the Service in the <i>Arar Report</i>.
Review 2007-04	<ul style="list-style-type: none"> • The Canadian Human Rights Commission not investigate this complaint in accordance with Subsection 46 (2) of the <i>Canadian Human Rights Act</i>. • The Minister provide the complainant with the opportunity to re-apply for the security clearance under the new policy. • If the complainant were to re-apply, CSIS or Transport Canada should conduct an interview with the complainant in the presence of counsel or other representative. In addition, the complainant should be made aware of the right to record the interview, and that CSIS or Transport Canada also record the interview and retain a copy of the recording until the complainant has had an opportunity to exhaust any review process or until the retention period under the <i>Privacy Act</i> has expired, whichever is later.

	SIRC recommended that...
Report 2007-05	<ul style="list-style-type: none">• CSIS prepare fresh advice to Citizenship and Immigration Canada that the presence of the complainant in Canada would not be detrimental to the national interest in accordance with Subsection 34(2) of the <i>Immigration and Refugee Protection Act</i>, or if required, could be used by the complainant to seek what is referred to as “Ministerial Relief.”
Report 2007-06	<ul style="list-style-type: none">• CSIS take all necessary steps to ensure the adoption of its <i>Security Screening Procedures Manual</i> and <i>Security Screening Investigator’s Guidebook</i> before June 30, 2008.• CSIS adopt guidelines to ensure that the information recorded and contained in the security screening database accurately reflect the status of the file to enable all users of the system to be as fully aware as possible of the file without having to review the hard-copy file, and that appropriate diary dates be included in its security screening database.• CSIS policy be revised as expeditiously as possible to prevent the destruction of recorded or written notes which may be required as evidence in proceedings before the courts or administrative tribunals.• CSIS provide its advice forthwith with regard to the complainant’s security assessment.

Le CSARS a recommandé...	
<ul style="list-style-type: none">• Que le SCRS rédige, à l'intention de Citoyenneté et Immigration Canada, un nouveau bref portant que la présence du plaignant au Canada ne sera pas préjudiciable à l'intérêt national, conformément au paragraphe 34(2) de la Loi sur l'immigration et la protection des réfugiés, ou destiné à servir au plaignant, au besoin, pour demander une exception dite « exception ministérielle ».	Rapport n° 2007-05
<ul style="list-style-type: none">• Que le SCRS prenne toutes les mesures nécessaires pour assurer l'adoption, avant le 30 juin 2008, de son Manuel des procédures de filtrage de sécurité et de son Guide de procédure à l'intention des enquêteurs de la Direction du filtrage de sécurité.• Que le SCRS adopte des lignes directrices pour assurer que l'information versée et contenue dans la base de données sur le filtrage de sécurité reflète avec exactitude l'état du dossier, afin que tous les utilisateurs du système puissent en connaître le contenu le plus possible sans devoir examiner le dossier sur papier, et que des échéances appropriées soient indiquées dans sa base de données sur le filtrage de sécurité.• Que la politique du SCRS soit revue le plus rapidement possible afin d'empêcher la destruction des notes enregistrées ou écrites qui pourraient être requises à titre de preuve dans des instances devant des tribunaux administratifs ou autres.• Que le SCRS donne ses conseils sur-le-champ au sujet de l'évaluation de sécurité du plaignant.	Rapport n° 2007-06

Résumé des recommandations du CSARS concernant les plaintes

Le CSARS a recommandé...	
Rapport n° 2007-01	<ul style="list-style-type: none"> • Que les politiques du SCRS soient modifiées de manière à permettre aux intéressés d'être accompagnés et pleinement représentés par un avocat ou par un autre représentant à une entrevue de filtrage de sécurité menée par le Service.
Rapport n° 2007-03	<ul style="list-style-type: none"> • Que le SCRS mette en œuvre les recommandations formulées à son intention dans le rapport Arar.
Rapport n° 2007-04	<ul style="list-style-type: none"> • Que la Commission canadienne des droits de la personne ne fasse pas enquête sur cette plainte, conformément au paragraphe 46(2) de la Loi canadienne sur les droits de la personne. • Que le Ministre donne au plaignant la possibilité de faire une nouvelle demande d'habilitation de sécurité selon la nouvelle politique. • Que, si le plaignant faisait une nouvelle demande, le SCRS ou Transports Canada l'interviewe en présence d'un avocat ou d'un autre représentant. De plus, le plaignant devrait être informé de son droit d'enregistrer l'entrevue et le SCRS ou Transports Canada devrait aussi l'enregistrer et conserver copie de l'enregistrement jusqu'à ce que le plaignant ait eu l'occasion d'épuiser tous ses recours ou jusqu'à l'expiration de la période de conservation prévue dans la Loi sur la protection des renseignements personnels, en retenant la dernière échéance.

Le CSARS a recommandé...	
Étude n° 2007-06	<ul style="list-style-type: none">• Que le débat quant à savoir si le groupe ciblé est en fait une organisation terroriste devrait entrer dans les discussions futures du SCRS sur le ciblage.
Étude n° 2006-08*	<ul style="list-style-type: none">• En ce qui a trait à l'enquête menée par le Service sur certains individus que l'on croit être des terroristes de deuxième génération ou des convertis de fraîche date aux interprétations extrémistes de l'islam, que le SCRS définisse clairement cette enquête contextuelle au prochain renouvellement et qu'il détermine si elle doit porter sur les questions qui sont sources d'inquiétudes croissantes. <p><small>* Note : Cette étude n'était pas terminée au moment de mettre sous presse le rapport annuel de 2006-2007.</small></p>

Résumé des recommandations du CSARS concernant les études

Le CSARS a recommandé...	
<ul style="list-style-type: none"> • Que les employés du SCRS établissent par écrit un relevé standard des renseignements non opérationnels échangés avec des partenaires étrangers. Ce relevé serait versé à la fois dans le dossier pertinent de « coopération avec » l'organisme en cause et dans la base de données opérationnelles. Il devrait aussi comporter des renvois aux renseignements opérationnels échangés avec ces partenaires étrangers. • Que, s'il coopère avec un organisme étranger, le Service conclue une entente distincte en vertu de l'article 17 avec cet organisme afin de se conformer à la <i>Loi sur le SCRS</i>, aux instructions ministérielles et aux politiques opérationnelles. 	<p>Étude n° 2007-01</p>
<ul style="list-style-type: none"> • Que le SCRS consulte le Secrétaire du Conseil du Trésor en vue de clarifier sa responsabilité de faire enquête sur les incidents signalés selon la Politique du gouvernement sur la sécurité, et d'explorer l'utilité d'améliorer la liaison interministérielle afin d'informer les ministères de leurs responsabilités en matière de filtrage de sécurité selon la politique. 	<p>Étude n° 2007-02</p>
<ul style="list-style-type: none"> • Que le SCRS revioie les critères guidant les évaluations de risques et définisse avec plus de précision les situations à niveau de risque élevé qui obligent à consulter le ministre de la Sécurité publique. 	<p>Étude n° 2007-04</p>
<ul style="list-style-type: none"> • Que le SCRS réexamine la structure de ses politiques afin de l'adapter à ses activités croissantes hors du Canada. • Que le SCRS normalise ses évaluations de risques par une terminologie détaillée et uniforme qui se reflète dans ses politiques opérationnelles. 	<p>Étude n° 2007-05</p>

Recommendations

Tableau 8 : Dépenses du CSARS 2007-2008		
	Dépenses réelles	Prévisions
Personnel	1 900 000 \$	1 844 000 \$
Biens et services	1 000 000 \$	781 000 \$
Total	2 900 000 \$	2 626 000 \$

DEMANDES EN VERTU DES LOIS SUR L'ACCÈS À L'INFORMATION ET SUR
LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le public peut présenter au CSARS des demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*. Le tableau 9 fait état du nombre de demandes que ces lois ont values au Comité au cours des trois derniers exercices financiers.

Tableau 9 : Demandes de communication de renseignements			
	2005-2006	2006-2007	2007-2008
Loi sur l'accès à l'information	17	12	15
Loi sur la protection des renseignements personnels	5	2	2

Dans le cadre de leur travail courant, le président et les membres du Comité ainsi que les cadres supérieurs prennent part régulièrement à des discussions avec la direction et le personnel du SCRS et avec d'autres membres de haut rang de la collectivité du renseignement de sécurité.

À ces échanges se greffent des discussions avec des universitaires, des experts en matière de sécurité et de renseignement et d'autres organismes compétents. Ces activités enrichissent le savoir du CSARS au sujet des questions et opinions qui influent sur le renseignement concernant la sécurité nationale.

Les membres du Comité visitent aussi les bureaux régionaux du Service à tout de rôle pour examiner l'incidence des instructions ministérielles et de la politique du SCRS sur le travail courant des enquêteurs locaux. Ces visites leur fournissent l'occasion de se faire renseigner par le personnel de ces bureaux sur les problèmes, difficultés et priorités qui leur sont propres. Elles leur permettent aussi de faire valoir ce qui polarise les efforts et les préoccupations du CSARS.

Au cours de 2007-2008, les membres du CSARS ont visité deux bureaux régionaux.

BUDGET ET DÉPENSES

Le CSARS continue de gérer ses activités dans les limites des ressources qui lui sont octroyées. Ses principales dépenses ont trait au traitement et aux déplacements de ses membres et de son personnel au Canada pour prendre part aux audiences, exposés et activités de surveillance du Comité. Le tableau 8 présente une ventilation des prévisions de dépenses et des dépenses réelles.

Activités du Comité

(suite)

20-21 septembre 2007 : Le directeur exécutif assiste à une conférence intitulée « Protecting Security and Human Rights: The Case of Migration in Canada », tenue à Ottawa par l'Institut de recherche en politiques publiques.

13 novembre 2007 et 31 mars 2008 : Le directeur exécutif donne une conférence sur le rôle et le mandat du CSARS à des étudiants inscrits à un cours de l'Université Carleton sur la sécurité nationale et le renseignement dans l'état moderne.

28 novembre 2007 : Le directeur exécutif et des cadres supérieurs rencontrent des représentants du Comité parlementaire norvégien de surveillance du renseignement.

30 novembre-2 décembre 2007 : Le directeur exécutif participe à titre d'expert à une conférence tenue par le comité du Justice Institute of British Columbia sur la diversité et le maintien de l'ordre. La conférence a pour titre « Balance between Security, Human Rights and Accountability ».

23 janvier 2008 : L'avocat principal est invité à prononcer une conférence sur le droit de la sécurité nationale à la Faculté de droit de l'Université d'Ottawa.

Au sujet du CSARS

COMPOSITION DU COMITÉ

La présidence du CSARS est occupée par l'honorable Gary Filmon, C.P., O.M., nommé à cette charge le 24 juin 2005. Les autres membres sont l'honorable Raymond Speaker, C.P., O.C., et l'honorable Roy Romanow, C.P., O.C., c.r.

Le mandat de l'honorable Baljit S. Chadha, C.P., a pris fin le 20 février 2008. Le 22 avril 2008, l'honorable Aldéa Landry, C.P., C.M., c.r., a remis sa démission du CSARS.

Tous les membres du Comité font partie du Conseil privé et sont nommés par le gouverneur en conseil après consultation entre le premier ministre et les chefs des partis de l'opposition.

En plus d'assister aux réunions mensuelles du Comité, les membres président les audiences de plaintes, préparent des études et des rapports de plaintes en consultation avec le personnel du CSARS, visitent les bureaux régionaux du SCRS, prennent la parole devant des comités parlementaires et exercent d'autres fonctions liées à leurs responsabilités.

PERSONNEL ET ORGANISATION

Le Comité jouit du soutien de son directeur exécutif, Susan Pollak, et d'un effectif autorisé de 20 employés, en poste à Ottawa. Son personnel est ainsi composé : un avocat principal, un conseiller principal, un directeur des services généraux, un avocat, un parajuriste principal (qui est aussi agent/analyste à l'accès à l'information et à la protection des renseignements personnels), plus des chercheurs et des employés de soutien administratif.

Les membres du Comité dictent au personnel l'orientation à donner aux travaux de recherche et aux autres activités qui sont désignées prioritaires pour l'année. La marche des affaires courantes est confiée au directeur exécutif qui s'enquiert au besoin de la ligne de conduite à tenir auprès du président, à titre de premier dirigeant.

Activités du Comité

23-25 mai 2007 : L'honorable Roy Romanow et l'avocat principal entretiennent les participants à un colloque marquant le 25^e anniversaire de la *Charte canadienne des droits et libertés* « A Living Tree: The Legacy of 1982 in Canada's Political Evolution », tenu par le Saskatchewan Institute of Public Policy.

7-8 juin 2007 : Le président, le directeur exécutif et un membre du CSARS assistent au colloque international des organismes de surveillance du renseignement sur la reddition de compte par les services de renseignement et de sécurité et sur les droits de la personne. Le président prononce une allocution devant les participants au colloque, tenu par le Review Committee on the Intelligence and Security Services et par la Faculté de droit de l'Université Radboud (Pays-Bas).

10-12 juin 2007 : Le président, les membres, le directeur exécutif et certains cadres assistent au Colloque international sur l'administration de la justice et la sécurité nationale dans les pays démocratiques, tenu à Ottawa par la Cour fédérale du Canada.

14 juin 2007 : Le directeur exécutif et des cadres supérieurs rencontrent l'inspecteur général de l'Australie.

18 juin 2007 : Le directeur exécutif, accompagné de cadres supérieurs, décrit devant un comité permanent du Sénat le rôle et les pouvoirs du CSARS à titre d'organisme de surveillance et de tribunal quasi judiciaire chargé d'entendre les plaintes.

Suite sur la page 56

Section 3

Au sujet du CSARS

- Appuyer la collecte de renseignements étrangers au Canada afin de prêter assistance au ministre des Affaires étrangères et/ou au ministre de la Défense nationale en vertu de l'article 16 de la *Loi sur le SCRS*;
- Exécuter les programmes de filtrage de sécurité pour les ministères et organismes fédéraux et pour d'autres clients;
- Fournir au gouvernement du Canada des évaluations du renseignement et veiller à ce que le SCRS se tienne au fait des contextes politiques, sociaux et économiques qui peuvent susciter des menaces à la sécurité du Canada;
- Veiller à ce que le matériel technique et les systèmes d'information du SCRS répondent aux besoins de ses enquêtes.

INSTRUCTIONS MINISTÉRIELLES

En vertu du paragraphe 6(2) de la *Loi sur le SCRS*, le ministre de la Sécurité publique peut donner des instructions écrites afin de guider les activités et enquêtes du Service. Ses dernières instructions remontent à 2001, année où un recueil a été remis au CSARS. En juillet 2008, celui-ci a toutefois reçu la dernière instruction du Ministre pour 2008-2009.

POLITIQUES OPÉRATIONNELLES DU SCRS

Les politiques administratives et opérationnelles du SCRS et celles qui ont trait à la sécurité et aux ressources humaines comportent des règles et des procédures qui régissent l'ensemble des activités du Service. Les politiques administratives et celles relatives à la sécurité et aux ressources humaines sont toutes d'ordre interne. Les politiques opérationnelles, qui décrivent la manière dont les employés du SCRS doivent exercer leurs fonctions, sont mises à jour régulièrement selon les changements apportés à la politique gouvernementale et ceux d'ordre législatif et autre.

En 2007-2008, le SCRS a révisé et/ou publié plus de 140 politiques. En outre, au-delà de 70 autres politiques ont été mises en place ou étaient en voie d'élaboration pendant la même période. Nombre de révisions étaient d'ordre administratif et les autres, d'ordre opérationnel, avaient notamment trait aux niveaux et au processus d'approbation des enquêtes ainsi qu'au filtrage de sécurité et aux pouvoirs prévus dans les mandats. De plus, dans le cadre d'un projet lancé par le directeur en 2006-2007, le Service a poursuivi son travail de révision de toutes les politiques opérationnelles afin de déterminer les cas où il lui faut déléguer les responsabilités de direction et de gestion.

RÈGLEMENTS ET NOMINATIONS PAR LE GOUVERNEUR EN CONSEIL

Selon le paragraphe 8(4) de la *Loi sur le SCRS*, le gouverneur en conseil peut établir, pour le Service, des règlements visant les pouvoirs et fonctions de son directeur ainsi que la conduite et la discipline de ses employés.

Le gouverneur en conseil n'a pris aucun règlement semblable en 2007-2008.

EXIGENCES NATIONALES EN MATIÈRE DE RENSEIGNEMENT
DE SÉCURITÉ

Le ministre de la Sécurité publique donne des instructions, appelées « Exigences nationales en matière de renseignement de sécurité », qui exposent les orientations générales du gouvernement quant aux plans sur lesquels le Service doit faire porter ses efforts d'enquête et qui le guident dans l'exercice de ses responsabilités en matière de collecte, d'analyse et de conseil.

Selon les Exigences nationales pour 2006-2008, le SCRS devait maintenir une capacité souple à répondre aux besoins de renseignements de sécurité qui se dessinent au Canada en tablant sur la gestion des risques. Le Ministère a noté que le contexte actuel de la menace a un caractère de plus en plus international et transnational, nombre de menaces à la sécurité du Canada émanant de l'extérieur du pays et obligeant à enquêter à l'étranger. Le SCRS a donc été invité à poursuivre ses enquêtes sur les menaces à la sécurité nationale tant au Canada qu'ailleurs dans le monde.

Pour 2006-2008, le Ministère a prescrit au SCRS de s'attacher aux priorités qui suivent en matière de renseignements de sécurité :

- Protéger contre la possibilité qu'une attaque terroriste survienne au Canada ou y prenne naissance ou qu'une telle attaque affecte des citoyens ou des biens canadiens à l'étranger, et conseiller le gouvernement à ce sujet;
- Poursuivre les recherches et analyses appuyant l'inscription des entités terroristes en vertu du *Code criminel* du Canada et lutter contre le financement du terrorisme;
- Soutenir les efforts du gouvernement du Canada en Afghanistan;
- Collaborer de façon étroite avec les autres ministères dans la lutte aux activités criminelles transnationales;
- Enquêter sur les menaces à la sécurité du Canada qui découlent d'activités de pays qui se livrent à l'espionnage;
- Poursuivre l'identification des pays et des groupes – et les enquêtes à leur sujet – qui possèdent des armes de destruction massive ou peuvent tenter d'en acquérir, et conseiller le gouvernement au sujet des menaces que constituent ces activités;

Des renseignements plus détaillés au sujet de ces programmes figurent sur le site Web de Transports Canada (www.tc.gc.ca).

ENTENTES AVEC DES ORGANISMES ÉTRANGERS

Le 31 mars 2008, le SCRS avait conclu 276 ententes avec des organismes de 147 pays. Toute nouvelle entente semblable doit être approuvée par le ministre de la Sécurité publique, en consultation avec son homologue des Affaires étrangères. Même en l'absence d'une telle entente, le SCRS peut quand même accepter les informations que lui fournissent spontanément les organismes ou organisations de pays étrangers. Le Ministère a approuvé cinq ententes nouvelles en 2007-2008 et il en a élargi trois qui existaient déjà.

En 2007-2008, le CSARS a examiné des ententes conclues avec des organismes étrangers et frappées de restrictions par le Service en raison des piteuses antécédents des pays ou organismes concernés en matière de droits de la personne, de leur fiabilité ou de leur capacité à protéger les renseignements fournis par le SCRS. En général, une entente frappée de restrictions fait que celui-ci ne peut échanger de renseignements opérationnels avec l'organisme en cause, même si elle ne l'empêche pas d'en accepter les informations qu'il lui fournit spontanément et qui concernent la sécurité du Canada.

Le CSARS a constaté que le SCRS a respecté les restrictions qu'il s'était lui-même imposées auprès des organismes concernés. Il a aussi constaté que le Service a su trouver un juste équilibre entre la nécessité de recueillir des renseignements vitaux en matière de sécurité et celle de demeurer à l'affût des problèmes que peut poser le fait de traiter avec un organisme frappé de restrictions.

C. Ententes avec des organismes étrangers et canadiens

Les articles 13 et 17 de la *Loi sur le SCRS* habiliteront le Service à conclure des ententes avec des organisations ou organismes canadiens et étrangers dans l'exercice de ses fonctions. Le CSARS reçoit copie de ces ententes à leur entrée en vigueur et il en examine un échantillon chaque année.

ENTENTES AVEC DES ORGANISMES CANADIENS

Le SCRS collabore souvent avec des ministères et organismes fédéraux, des gouvernements provinciaux et des services de maintien de l'ordre. Depuis le 11 septembre, davantage de groupes s'occupent de sécurité nationale, dont les forces de police et d'autres partenaires du secteur public. Cela représente un défi pour le Service, car il doit cultiver de saines relations avec tous ses partenaires, tant anciens que nouveaux, pour s'assurer de l'efficacité à la fois des échanges d'information et de la conduite des opérations conjointes.

Nombre d'accords conclus avec des organismes canadiens prennent la forme de protocoles d'entente, mais le SCRS peut collaborer avec eux sans conclure de protocole d'entente.

Le 31 mars 2008, le SCRS avait conclu 39 protocoles d'entente avec des partenaires canadiens : 29 avec des ministères ou organismes fédéraux et 10 avec des entités provinciales et municipales.

En 2007-2008, le CSARS a examiné une entente du Service avec Transports Canada, mettant l'accent sur l'apport de renseignements tirés du filtrage de sécurité par le Service à l'appui de deux programmes de ce ministère : le Programme d'habilitation de sécurité en matière de transport maritime et le Programme de protection des passagers. Transports Canada est chargé de veiller à ce que le réseau national de transport aérien, maritime, ferroviaire et routier soit sécuritaire, efficace et accessible.

Pour ce qui est du Programme d'habilitation de sécurité en matière de transport maritime, le CSARS a constaté que, même s'il n'est pas encore pleinement en vigueur, le SCRS a collaboré avec Transports Canada, afin d'atténuer le risque des menaces à la sécurité, à vérifier les antécédents de ceux qui travaillent dans les installations maritimes et qui ont accès à certaines zones ou remplissent certaines fonctions. Quant au Programme de protection des passagers, le CSARS a constaté que le SCRS s'est employé efficacement, avec Transports Canada (de concert avec la GRC, qui contribue aussi au Programme), à s'assurer que les individus inscrits sur la liste dite des « personnes interdites de vol » constituent vraiment une menace pour la sécurité de l'aviation, et que les décisions de porter les noms d'individus sur cette liste reposent sur des critères clairement définis.

COMMUNICATION D'INFORMATIONS

L'article 19 de la *Loi sur le SCRS* interdit la communication d'informations obtenues par le Service dans le cadre d'enquêtes, sauf dans des circonstances particulières. Le SCRS peut ainsi communiquer des informations :

1. pouvant servir dans le cadre d'une enquête ou de poursuites relatives à une infraction présumée à une loi fédérale ou provinciale, et cela, aux agents de la paix compétents pour mener l'enquête, au ministre de la Sécurité publique et au procureur général de la province concernée;
2. concernant la conduite des affaires étrangères du Canada, et cela, au ministre des Affaires étrangères;
3. concernant la défense du Canada, et cela, au ministre de la Défense nationale;
4. essentielles pour des raisons d'intérêt public, selon le Ministre, et cela, à un ministre ou à un fonctionnaire fédéral.

Il importe de noter que l'alinéa 19(2)d) habilite le ministre de la Sécurité publique à passer outre à toute crainte de violation de la vie privée et à autoriser le SCRS à communiquer des informations réputées être dans l'intérêt national ou public. Si de telles informations sont divulguées, le directeur du SCRS doit en faire rapport au CSAARS, ce qui est extrêmement rare : il n'y a eu que deux cas de communications visées par cet alinéa.

Le Service peut aussi communiquer des informations, par écrit ou verbalement, aux organismes d'exécution de la loi ou aux entités fédérales, tels que le ministère de la Défense nationale et Affaires étrangères Canada. Lorsque le SCRS autorise la GRC à utiliser ses informations dans des instances judiciaires, il doit le faire par écrit.

Le Service a présenté plus de 90 notes de communication au cours de l'exercice 2007-2008.

CERTIFICAT DE L'INSPECTEUR GÉNÉRAL DU SCRS (2006-2007)

La fonction d'inspecteur général du SCRS a été établie en 1984, en vertu de la *Loi sur le SCRS*, à titre de « vigile » du ministre de la Sécurité publique, chargé d'examiner les opérations du Service et de fournir l'assurance que celui-ci se conforme aux instructions ministérielles, aux politiques opérationnelles et à la *Loi sur le SCRS*.

Chaque année, l'inspecteur général remet au Ministre un certificat attestant de la mesure où il est satisfait du rapport annuel du directeur du SCRS. Dans ce certificat, il informe de tout cas où le Service aurait exercé ses pouvoirs de façon abusive ou inutile et où il ne se serait pas conformé à la *Loi sur le SCRS* ou aux instructions ministérielles.

Dans son dernier certificat, l'inspecteur général s'est dit satisfait du rapport annuel du directeur du SCRS pour 2006-2007, affirmant que le Service n'a pas outrepassé les pouvoirs que lui confère la loi, qu'il n'a dérogé à aucune instruction ministérielle et qu'il n'a pas exercé ses pouvoirs d'une façon abusive ou inutile.

Cependant, l'inspecteur général s'est dit préoccupé par le nombre croissant de cas de non-conformité à la politique du SCRS sur les opérations et par la multiplication des erreurs de transcription dans les documents. La plupart des cas de non-conformité étaient des erreurs administratives. L'inspecteur général a aussi fait observer le temps qui avait été requis pour élaborer ou mettre à jour les politiques opérationnelles afin de faire face à l'évolution des exigences et des activités.

Pour de plus amples renseignements sur le certificat de l'inspecteur général du SCRS, prière de consulter le site Web de la Sécurité publique (www.securitepublique.gc.ca).

AGISSEMENTS ILLICITES DU SCRS

En vertu du paragraphe 20(2) de la *Loi sur le SCRS*, le directeur du Service doit présenter un rapport au Ministre s'il est d'avis qu'un employé du SCRS peut avoir commis un acte illicite dans l'exercice de ses fonctions. Le cas échéant, le Ministre doit alors transmettre ce rapport au procureur général du Canada et au Comité, en y joignant ses observations. En 2007-2008, aucun employé du SCRS n'a commis d'acte illicite et aucun rapport semblable n'a été présenté.

B. Exigences en matière de rapports

RAPPORT ANNUEL DU DIRECTEUR DU SCRS (2006-2007)

Chaque année, le directeur du SCRS présente au ministre de la Sécurité publique un rapport classifié qui décrit en détail les priorités et les activités opérationnelles du Service. L'inspecteur général du SCRS examine ce rapport et remet au Ministre un certificat attestant de la mesure où il est satisfait de son contenu. Par la suite, le Ministre envoie copie des deux documents au CSARS afin qu'il les examine, tel qu'il est prescrit à l'alinéa 38a) de la *Loi sur le SCRS*.

Dans l'édition 2006-2007 du rapport, la première depuis la réorganisation des ressources opérationnelles au sein du SCRS, le directeur a noté que la réorganisation confère au Service une structure organisationnelle souple qui peut être facilement modifiée selon les besoins opérationnels futurs.

En plus de résumer l'utilisation des sources humaines par le Service durant l'année, le rapport fait état des activités de chaque direction opérationnelle et de tout groupe spécialisé du SCRS, ainsi que de toutes les ententes conclues avec des organismes canadiens et étrangers, tel qu'il est prévu à l'article 17 de la *Loi sur le SCRS*.

Le directeur a signalé que le SCRS avait suspendu ses relations avec cinq sources humaines pour raison d'activité criminelle. Il a en outre noté que le SCRS n'avait pas ordonné aux sources de mener cette activité et qu'il a immédiatement pris des mesures correctives en apprenant les incidents. Le directeur a souligné le rôle du SCRS pour ce qui est d'identifier le présumé espion russe Paul William Hampel et aussi de l'expulser du Canada. Le directeur a aussi signalé que la Direction du Moyen-Orient et de l'Afrique du Service avait mis fin à une enquête fautive de rapports d'activités liées à la menace.

À noter, en particulier, que le directeur a porté à l'attention du ministre de la Sécurité publique les difficultés auxquelles se heurte le SCRS par suite de la croissance rapide des technologies liées à Internet et des changements qui s'y rapportent. Il a mentionné qu'une solution à ces difficultés serait que le Parlement adopte un projet de loi comme celui sur l'aide technique aux services de police, qui avait été déposé en novembre 2005 mais n'avait pas été adopté par suite du déclenchement de l'élection fédérale tout de suite après.

Le lecteur est prié de noter que le SCRS affiche les rapports publics non classifiés sur son site Web (www.csis-scrs.gc.ca).

MANDATS DE LA COUR FÉDÉRALE : GÉNÉRALITÉS ET STATISTIQUES

Mis à part leur caractère fort intrusif, les mandats sont l'un des instruments les plus puissants qui soient à la portée du SCRS. Par ce moyen, la Cour fédérale l'autorise à employer des méthodes d'enquête qui seraient autrement illégales, comme l'interception de communications téléphoniques. Pour cette raison, le recours aux mandats par le Service représente un important volet des études du CSARS.

Chaque année, le CSARS recueille des statistiques sur les demandes de mandats du Service et sur les mandats que la Cour fédérale décerne à celui-ci en vertu des articles 12 et 16 de la *Loi sur le SCRS*. Le CSARS n'examine pas tous les aspects de ces mandats, en raison notamment du fait que cela entre dans la fonction vitale de responsabilité qui est assurée par la Cour fédérale. Cependant, dans le cadre de ses activités de surveillance, il examine bel et bien si le Service se conforme aux mandats décernés par la Cour fédérale (c.-à-d. qu'il se penche sur la manière dont le SCRS exerce les pouvoirs prévus dans les mandats).

En 2007-2008, la Cour fédérale a approuvé 71 mandats nouveaux, ce qui représente une augmentation notable par rapport à l'exercice précédent. Elle a aussi approuvé le remplacement ou le renouvellement de 182 mandats, autre hausse par rapport au chiffre de l'exercice précédent. Pendant la même période, 56 mandats ont été suspendus ou ont pris fin sans être renouvelés. La Cour fédérale n'a rejeté aucune demande de mandat. Dans un cas, elle a rejeté la demande du Service visant à être autorisé à intercepter les communications de sujets d'une enquête hors du Canada. Dans sa décision, la Cour a statué qu'elle n'avait pas compétence pour décerner le mandat demandé en vertu de la *Loi sur le SCRS*.

Tableau 7
Statistiques sur les mandats

	2004-2005	2005-2006	2006-2007	2007-2008
Mandats nouveaux	40	24	42	71
Mandats remplacés ou renouvelés	207	203	134	182
Total	247	227	176†	253††

† Comprend 25 mandats urgents.
†† Comprend 19 mandats urgents.

ii. Opérations

Au sein des Opérations, quatre directions ont charge d'enquêter sur les diverses menaces qui émanent de leur zone respectue, à l'exception de la Direction du terrorisme international qui se concentre exclusivement sur Al-Qaïda et sur les groupes dans sa mouvance, indépendamment des frontières géographiques.

Direction du Moyen-Orient et de l'Afrique

Cette direction concentre ses enquêtes sur les menaces qui émanent des pays du Moyen-Orient et de l'Afrique ou dont ces pays sont les principaux foyers. Cela englobe les questions du terrorisme, des activités influencées par l'étranger, de la prolifération des armes de destruction massive et de l'espionnage.

Direction de l'Asie, de l'Europe et des Amériques

Cette direction enquête sur les menaces qui émanent de la vaste zone dont elle a la charge, à savoir l'espionnage, le terrorisme (y compris l'extrémisme intérieur), les activités criminelles transnationales et celles qui sont influencées par l'étranger.

Direction du terrorisme international

Cette direction enquête dans tous les pays du monde, dont le Canada, mettant l'accent sur les extrémistes islamistes qui se livrent à diverses activités liées au terrorisme et menaçant directement les Canadiens et les intérêts canadiens. Entre autres domaines d'intérêt notables de cette direction figure la radicalisation des islamistes au Canada.

Région internationale

Cette direction gère la liaison avec les organismes étrangers et coordonne les visites de représentants étrangers à l'Administration centrale et aux bureaux régionaux du SCRS. Elle a aussi charge de coordonner toutes les ententes conclues avec des services étrangers de renseignement de sécurité ou d'exécution de la loi en vertu du paragraphe 17(1), ainsi que le fonctionnement des bureaux d'agent à l'étranger du Service. Celui-ci mise sur ces bureaux pour aider à assurer la liaison avec les services étrangers de la sécurité et du renseignement et pour coordonner les visites de représentants étrangers à l'Administration centrale et aux bureaux régionaux du SCRS.

DIRECTION DES SOURCES HUMAINES ET DU SOUTIEN
AUX OPÉRATIONS

Cette direction assure un éventail de services de soutien et de coordination, dont la gestion des risques et un service d'analyse des activités opérationnelles à l'échelle du Service. Elle est le centre stratégique dans divers domaines, y compris la sécurité des opérations, les services multilingues et la gestion des sources humaines. Elle englobe aussi le Centre de gestion des menaces qui assure un soutien 7 jours par semaine, 24 heures par jour, au personnel opérationnel de l'Administration centrale et des bureaux régionaux et aux agents à l'étranger. De plus, elle soutient le Service dans sa participation aux événements spéciaux importants, tels le Sommet des leaders nord-américains de l'an dernier et les prochains Jeux olympiques d'hiver, qui se tiendront à Vancouver en 2010.

DIRECTION DES SERVICES TECHNIQUES ET SCIENTIFIQUES

Cette direction élabore et déploie des outils et mécanismes techniques afin de soutenir les opérations et enquêtes des autres directions du SCRS.

CENTRE INTÉGRÉ D'ÉVALUATION DES MENACES

Le Centre intégré d'évaluation des menaces (CIEM) produit des évaluations qui servent à alerter le gouvernement à propos des menaces terroristes pesant sur le Canada et sur les intérêts canadiens à l'étranger. Ces évaluations sont distribuées aux partenaires canadiens et étrangers. De plus, le CIEM est la plaque tournante des évaluations de la menace qui émanent de ses pendants aux États-Unis, au Royaume-Uni, en Australie et en Nouvelle-Zélande.

Pendant la période considérée, le CIEM a effectué 348 évaluations de la menace et il en a redistribué plus de 1 300 autres émanant de centres de fusion alliés. Il a aussi publié *Coup d'œil sur les médias* à chaque jour ouvrable afin de le distribuer à ses clients. En outre, le CIEM a donné plus de 120 exposés à ses clients canadiens, entre autres au Séminaire annuel sur la sécurité de l'industrie pétrolière, à la conférence de liaison de l'Association canadienne des chefs de police, au Groupe de travail sur la cybersécurité et à une conférence sur les infrastructures essentielles aux États-Unis.

Pendant la période considérée, le CIEM a assumé la responsabilité de la Sous-section des évaluations de la menace, qui produit des évaluations périssables sur d'éventuelles menaces à l'endroit des Canadiens et des intérêts canadiens au Canada ou à l'étranger, ou sur les intérêts ou ressortissants étrangers au Canada. Le CIEM a fourni des évaluations de problèmes clés au gouvernement du Canada et relativement à la tenue du Sommet des leaders nord-américains en août 2007, à Montebello, au Québec. Il est aussi à noter qu'il a rédigé trois communications en collaboration avec le Canadian Centre for Intelligence Studies de l'Université Carleton.

Le CIEM a poursuivi son travail de planification en vue d'un centre fonctionnant 7 jours par semaine, 24 heures par jour, et doté d'une capacité d'analyse intégrée.

Autres activités de filtrage

En 2007-2008, la Direction du filtrage de sécurité a aussi étudié 11 300 demandes de visa pour les programmes étrangers. De plus, elle a pris part aux deux programmes suivants :

- **Voyageurs dignes de confiance** – programme de prédédonnement, actuellement en voie d'élaboration, destiné aux voyageurs qui vont souvent aux États-Unis;

- **Protection des passagers** – avec d'autres ministères, la Direction s'est employée à élaborer des programmes de contrôle des passagers de lignes aériennes, en particulier le programme intérieur des « personnes interdites de vol » qui est entré en vigueur le 18 juin 2007.

DIRECTION DE L'ÉVALUATION DU RENSEIGNEMENT

La Direction de l'évaluation du renseignement regroupe la fonction d'analyse clé du Service et en centralise les principaux mécanismes de rapports de renseignement. Elle élabore des analyses stratégiques et opérationnelles des menaces existantes et des problèmes nouveaux, et produit des évaluations du renseignement, des évaluations de la menace et des risques ainsi que *Perspectives*.

Ces dernières années, la Direction a opéré une série de changements dans le but de répondre à la demande croissante d'évaluations stratégiques et opérationnelles au sein du Service et à l'échelle du gouvernement. Dans le cadre de ce processus, la Direction a amorcé un dialogue avec ses partenaires et ses clients fédéraux en vue d'assurer que le SCRS continue de fournir à point nommé à ses clients des évaluations pertinentes répondant à leurs besoins. Elle a cherché des occasions de coordination, avec ses partenaires de la collectivité de l'évaluation, afin de cerner les domaines d'intérêt commun et de produire des évaluations de la collectivité. De même, la Direction a créé des mécanismes internes visant à promouvoir un dialogue constant avec les agents du Service chargés de la collecte pour assurer la prestation en temps utile d'un soutien analytique destiné à appuyer les enquêtes.

Cette direction joue aussi un rôle dans le processus de la liste des entités terroristes, à la fois pour ce qui est d'y inscrire de nouvelles entités et d'y maintenir celles dont les noms y figurent déjà. Le Service prépare des rapports de renseignement de sécurité sur les groupes que l'on croit être des entités terroristes ou agir au nom de telles entités. Dans ces rapports, il énonce ses constatations et c'est sur eux que s'appuie l'examen du gouverneur en conseil visant à déterminer s'il y a lieu d'approuver l'inscription d'un groupe en vertu de l'article 83.05 du *Code criminel* du Canada. Selon le *Code criminel*, le ministre de la Sécurité publique est tenu d'examiner la liste des entités terroristes tous les deux ans pour déterminer s'il subsiste des motifs raisonnables d'y maintenir des entités, et de faire une recommandation en conséquence au gouverneur en conseil.

L'examen le plus récent de la liste par le Ministère a été entrepris en février 2008 et doit prendre fin cet automne.

Le SCRS ne trouve aucun renseignement défavorable dans la majorité de ses enquêtes de filtrage de candidats au statut de réfugié, à l'immigration ou à la citoyenneté. En 2007-2008, il a présenté 325 notes de brefage, 129 brefs d'interdiction de territoire et 1 lettre d'information accessoire à l'égard de dossiers d'immigration.

Ces dernières années, les délais médians de remise de notes de brefage ou de brefs d'interdiction de territoire par le Service ont en général été assez longs. En 2007-2008, il a été de 508 jours civils pour les demandes de notes de brefage présentées au Canada à l'égard de dossiers d'immigration, de 620 jours pour celles provenant des États-Unis et de 150 jours pour celles émanant de l'étranger. Pour les notes de brefage concernant les demandeurs de résidence permanente qui étaient réfugiés au Canada, le délai de traitement médian a été de 497 jours, et de 339 jours pour les demandes relatives aux dossiers du Contrôle de sécurité préliminaire.

Le tableau 6 présente un relevé triennal des délais médians du Service à fournir des avis de vérification de données.

Tableau 6
Délais médians (en jours) à fournir des avis de vérification de données

	2005-2006	2006-2007	2007-2008
Citoyenneté	1	1	1
Immigration (Canada) [†]	70	78	59
Immigration (États-Unis) ^{††}	62	29	45
Immigration (de l'étranger)	16	14	20
Détermination du statut de réfugié	96	98	64
Contrôle de sécurité préliminaire	23	19	28

[†] Comprend certaines catégories de personnes qui demandent, au Canada, le statut de résident permanent.
^{††} Comprend les personnes qui sont admises légalement au Canada depuis au moins un an et qui peuvent présenter leurs demandes aux bureaux de Citoyenneté et Immigration aux États-Unis.

Le **Filtrage à l'immigration** aide à veiller à ce que les individus qui posent une menace à la sécurité et/ou qui sont interdits de territoire selon la LIPR ne puissent entrer au Canada ni y obtenir un statut. Ce programme donne lieu à des avis touchant la sécurité et permettant :

- a) de déterminer si les demandeurs de citoyenneté se livreront, entre autres, à des activités qui constituent une menace à la sécurité du Canada;
- b) d'identifier les individus qui sont interdits de territoire pour l'une des raisons de sécurité énumérées au paragraphe 34(1) de la LIPR;
- c) d'identifier les individus qui demandent le statut de visiteur ou de réfugié à des points d'entrée au Canada et qui sont interdits de territoire pour raisons de sécurité;
- d) d'écarter les demandeurs de visas de visiteurs qui viennent de pays posant une menace sur le plan du terrorisme, de l'espionnage et des activités criminelles transnationales.

En 2007-2008, la Direction a reçu 94 400 demandes en vertu des divers programmes de filtrage à l'immigration (voir le tableau 5). Le nombre de demandes reçues tant du Canada que de l'extérieur était voisin de celui de l'exercice précédent, tandis que celui des demandes de détermination du statut de réfugié a diminué. Le nombre de demandes de contrôle de sécurité préliminaire était plus élevé que celui de l'exercice précédent.

Tableau 5
Filtrage de sécurité à l'immigration

	Demandes			Notes ou brefs		
	2005-2006	2006-2007	2007-2008	2005-2006	2006-2007	2007-2008
Au Canada et à l'étranger [†]	63 200	62 800	66 000	133	201	195
Contrôle de sécurité préliminaire ^{††}	17 100	17 900	21 800	89	143	117
Détermination du statut de réfugié ^{†††}	11 700	11 600	6 600	127	153	142
Total partiel	92 000	92 300	94 400	349	497	454
Demandes de citoyenneté	308 000	227 300	190 000	120	155	109
Total	400 000	319 600	284 400	469	652	563

* Chiffres arrondis à la centaine la plus proche.

[†] Comprend les demandes de résidents permanents au Canada et à l'étranger (à l'exclusion du Programme de détermination du statut de réfugié), de résidents permanents aux États-Unis et de demandeurs à l'étranger.

^{††} Dans les cas de demandes de statut de réfugié présentées au Canada ou à des points d'entrée.

^{†††} Les réfugiés, au sens de la LIPR, qui présentent au Canada une demande de statut de résident permanent.

d'octroyer, de retirer ou de refuser l'habilitation. En 2007-2008, le Service a remis huit notes de breffage contenant des renseignements défavorables et deux avis de refus.

Le SCRS fournit aussi des évaluations de sécurité en vue de l'accès à des sites particuliers (voir le tableau 4). Contrairement à la core de sécurité du gouvernement, ce type d'autorisation permet à son détenteur d'accéder à certaines zones sécurisées ou l'accrédite en vue d'un événement spécial. En 2007-2008, le SCRS a reçu plus de 67 500 demandes de filtrage de ce type et il n'a fourni aucune note de breffage aux organismes demandeurs. L'augmentation des demandes d'accès aux centrales nucléaires en 2006-2007 est l'aboutissement d'un cycle quinquennal de renouvellement des habilitations existantes. Le nombre de ces demandes a donc diminué en 2007-2008. Il y a aussi eu diminution du nombre de demandes associées au programme Expéditions rapides et sécuritaires (EXPRES).

Le Service a fourni plus de 1 300 évaluations en vue d'événements spéciaux en 2007-2008.

Tableau 4
Filtrage concernant l'accès à des sites*

	2005-2006	2006-2007	2007-2008
Cité parlementaire	1 000	1 100	1 100
Zones réglementées d'aéroports	37 600	39 300	36 800
Centrales nucléaires	10 600	17 900	9 200
Expéditions rapides et sécuritaires (EXPRES)	3 100	23 100	10 700
Accréditation en vue d'événements spéciaux	5 600	0	1 300
Programme d'habilitation de sécurité en matière de transport maritime†	S.O.	S.O.	6 300
Autres ministères	2 400	2 500	2 100
Total	60 300	83 900	67 500

* Chiffres arrondis à la centaine la plus proche.

† Le Programme d'habilitation de sécurité en matière de transport maritime, entré en vigueur en décembre 2007, vise à fournir des évaluations relatives à la sécurité des ports du Canada.

Dans ses efforts pour jauger son efficacité à répondre aux demandes de filtrage de sécurité, le SCRS calcule les délais d'exécution en nombres médians de jours civils. Comme le montre le tableau 3, les délais médians ont diminué par rapport à ceux de l'exercice précédent, sauf dans le cas des habilitations de niveau III (Très secret) où ils ont allongé. Cependant, les délais médians pour cette catégorie ont été calculés différemment en 2007-2008, ce qui a donné une augmentation des délais médians comparativement aux exercices précédents. Pour 2007-2008, les délais médians pour les habilitations de niveau III excluent les mises à jour pour les personnes détenant déjà cette habilitation, processus qui nécessite un délai sensiblement moindre que les demandes d'habilitations nouvelles ou rehaussées⁵.

Par exemple, le délai médian pour une habilitation nouvelle ou rehaussée de niveau III du MDN est de 164 jours, mais de 29 jours pour une mise à jour. De la même façon, pour les clients autres que le MDN, le délai médian est de 186 jours pour une habilitation nouvelle ou rehaussée de niveau III, contre 4 jours pour une mise à jour.

Tableau 3
Délais médians (en jours civils)

MDN	Autres que le MDN			MDN			
	Niveau I (Confidentiel)	Niveau II (Secret)	Niveau III (Très secret)	2005-2006	2006-2007	2007-2008	
	24	19	39	40	40	28	164 (nouvelles) 29 (mises à jour)
	24	15	60	47	21	13	186 (nouvelles) 4 (mises à jour)

Le Service ne décide pas qui doit se voir octroyer une habilitation de sécurité. Il fait plutôt part, au ministre ou à l'organisme demandeur, des renseignements susceptibles d'influer sur la décision de celui-ci d'en octroyer une ou non. Rares sont les occasions où le SCRS l'avise que le critère de la Politique du gouvernement sur la sécurité est rempli, obligeant à refuser l'habilitation. Il appartient toutefois à l'organisme demandeur

⁵ Les titulaires d'habilitations de niveau III (Très secret) doivent renouveler/mettre à jour leur niveau d'habilitation tous les cinq ans. Les évaluations en vue d'habilitations nouvelles ou rehaussées comprennent les demandes d'habilitation et les demandes d'habilitation d'un niveau plus élevé (p. ex., le titulaire d'une habilitation de niveau I qui en demande une de niveau III).

Le programme de **filtrage pour le gouvernement** amène le Service à fournir des évaluations de sécurité qui servent à jauger la loyauté des intéressés envers le Canada quant à leur habilité personnelle et qui sont fournies à tous les ministères et institutions du gouvernement, à l'exception de la Gendarmerie royale du Canada (GRC) pour laquelle le SCRS effectue des vérifications dans ses fichiers et à l'étranger, dont des entrevues personnelles conjointes pour un motif valable. Le Service prend aussi part à un programme d'autorisation d'accès aux aéroports, aux ports et aux installations maritimes, à la cité parlementaire et aux centrales nucléaires, et il fournit des évaluations aux ministères provinciaux. Ces programmes visent à renforcer la sécurité et à réduire le risque que représentent les groupes terroristes et les gouvernements étrangers qui cherchent à avoir accès à des informations classifiées ou à d'autres biens, matériels et sites sensibles.

Depuis toujours, les clients qui recourent le plus à ce service sont Travaux publics et Service gouvernementaux Canada et le ministère de la Défense nationale (MDN), qui regroupent respectivement 30 et 16 p. 100 de toutes les demandes en 2007-2008.

Comme le montre le tableau 2, le SCRS a reçu 50 300 demandes d'habilitations de sécurité, nouvelles ou mises à jour en 2007-2008, et il a fourni 48 800 évaluations de sécurité aux ministères fédéraux. Le nombre des demandes a légèrement fléchi par rapport à l'exercice précédent, tout comme celui des évaluations de sécurité. Le changement le plus grand a été une diminution du nombre de demandes du MDN.

Tableau 2
Filtrage de sécurité du SCRS pour le gouvernement*

	2005-2006	2006-2007	2007-2008
Demandes du MDN	9 200	13 100	8 800
Demandes d'autres ministères et organismes	32 900	38 100	41 500
Total	42 100	51 200	50 300
Evaluations fournies au MDN	8 900	13 100	8 300
Evaluations fournies aux autres ministères et organismes†	28 900	41 800	40 500
Total	37 800	55 000	48 800

* Chiffres arrondis à la centaine la plus proche.
† Comprend les évaluations effectuées pour les gouvernements provinciaux et pour l'accès aux centrales nucléaires.

i. Renseignement

DIRECTION DU FILTRAGE DE SÉCURITÉ

À titre d'élément clé du cadre de la sécurité nationale du Canada, la Direction du filtrage de sécurité exerce l'une des fonctions les plus en vue du Service.

La Direction du filtrage de sécurité comporte deux volets centraux touchant, l'un le gouvernement et l'autre, l'immigration. Face au nombre croissant de demandes de filtrage reçues ces dernières années, la Direction s'est employée à améliorer sa fonction technique et celle de la gestion de cas de manière à continuer de fournir à point nommé à ses clients des évaluations pertinentes et exactes qui répondent à leurs attentes. La Direction a aussi consulté ses clients ministériels afin de les guider dans l'application de nouvelles règles concernant le processus de filtrage de sécurité.

Les conseils du SCRS concernant le filtrage de sécurité peuvent prendre l'une ou l'autre des cinq formes suivantes :

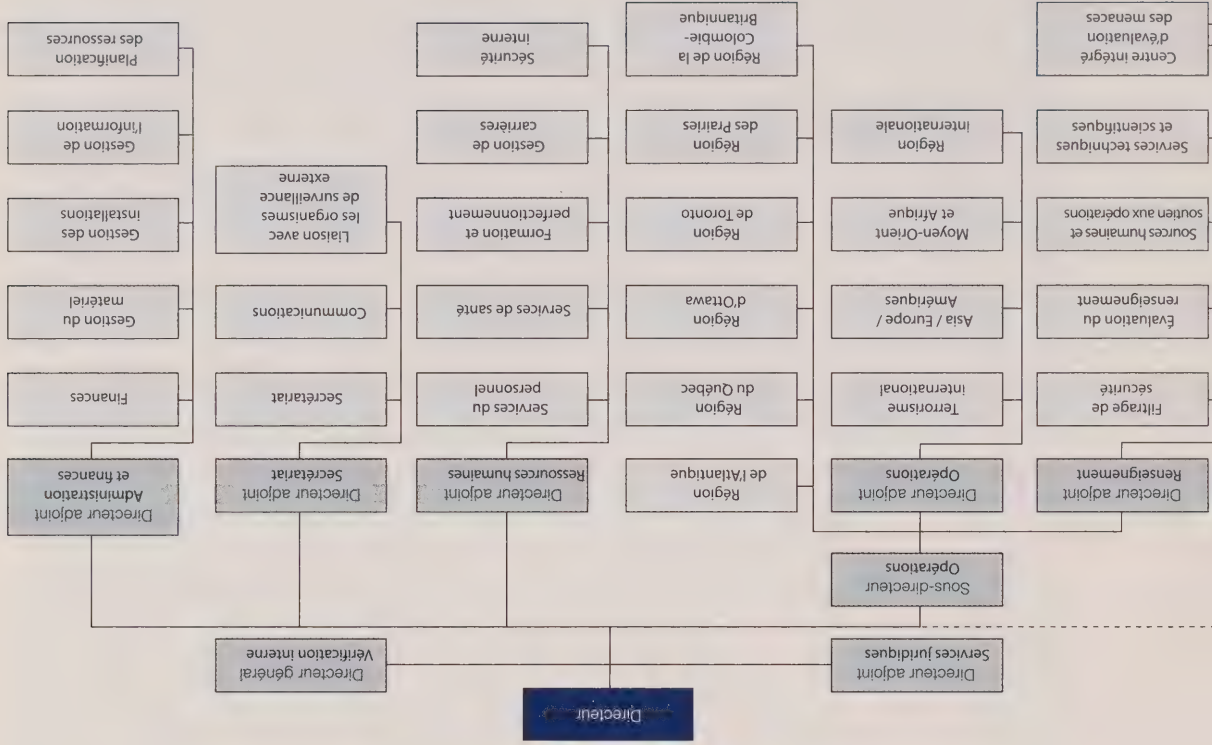
1. **Avis de vérification de données** : remis dans les cas de filtrage pour le gouvernement et l'immigration si le SCRS ne trouve aucun renseignement défavorable au sujet du demandeur.
2. **Lettre d'information accessoire** : fournie à Citoyenneté et Immigration Canada (CIC) et à l'Agence des services frontaliers du Canada (ASFC) si le Service a des renseignements au sujet d'un demandeur qui prend ou a pris part à des activités étrangères à la sécurité, décrites dans la *Loi sur l'immigration et la protection des réfugiés* (LIPR).
3. **Note de breffage** : remise dans les cas de filtrage pour le gouvernement si le SCRS a des informations qui pourraient influencer la décision de l'organisme demandeur d'octroyer à un candidat une habilitation de sécurité ou d'accès à un site. Aussi remise dans les dossiers de filtrage à l'immigration si le Service a des informations voulant que le candidat trempe ou ait trempe dans des activités qui n'emportent pas nécessairement contre lui interdiction de territoire au Canada.
4. **Bref d'interdiction de territoire** : fourni à CIC ou à l'ASFC si le SCRS croit que le demandeur est interdit de territoire au Canada, selon les dispositions de la LIPR relatives à la sécurité.
5. **Avis de refus** : remis dans les cas où le Service recommande à l'organisme demandeur de refuser au candidat une habilitation de sécurité ou d'accès à des sites.

A. Activités opérationnelles du SCRS

Le sous-directeur, Opérations, qui relève du directeur du SCRS, a charge de trois groupes :

- le **Renseignement**, qui compte cinq directions (Filtrage de sécurité, Évaluation du renseignement, Sources humaines et Soutien aux opérations, Services techniques et scientifiques, et Centre intégré d'évaluation des menaces);
- les **Opérations**, composées de trois directions et d'une région (Terrorisme international, Moyen-Orient et Afrique, et Asie, Europe et Amériques, ainsi que Région internationale);
- **six régions**.

Service canadien du renseignement de sécurité



Section 2

Activités opérationnelles et mécanismes
redditionnels du SCRS

Le CSARS a formulé quatre recommandations :

- que le SCRS prenne toutes les mesures nécessaires pour assurer l'adoption, avant le 30 juin 2008, de son *Manuel des procédures de filtrage de sécurité* et de son Guide de procédure à l'intention des enquêteurs de la Direction du filtrage de sécurité;
- que le SCRS adopte des lignes directrices pour assurer que l'information versée et contenue dans la base de données sur le filtrage de sécurité reflète avec exactitude l'état du dossier, afin que tous les utilisateurs du système puissent en connaître le contenu le plus possible sans devoir examiner le dossier sur papier, et que des échéances appropriées soient indiquées dans sa base de données sur le filtrage de sécurité;
- que la politique du SCRS soit revue le plus rapidement possible afin d'empêcher la destruction des notes enregistrées ou écrites qui pourraient être requises à titre de preuve dans des instances devant des tribunaux administratifs ou autres;
- que le SCRS donne ses conseils sur-le-champ au sujet de l'évaluation de sécurité du plaignant.

La deuxième constatation a trait à la destruction des notes de l'enquêteur du SCRS. Le CSARS a été informé qu'il avait détruit les notes prises à l'entrevue avec le plaignant, selon la politique du SCRS sur les opérations OPS-217, intitulée *Notes opérationnelles*, et donc qu'elles ne pouvaient être mises à sa disposition pour l'enquête. Le CSARS a établi que la destruction des notes n'avait pas nui à son enquête. Il a toutefois conclu que les notes d'entrevue de filtrage à l'immigration peuvent être requises à titre de preuve ou d'information pour des enquêtes ou des poursuites devant la Cour ou les tribunaux administratifs et, en conséquence, que le Service devrait les conserver. Le CSARS avait recommandé en d'autres occasions de ne pas détruire les notes d'entrevue. Enfin, le CSARS a recommandé que le SCRS rédige, à l'intention de CIC, un nouveau bref qui puisse convaincre le Ministre que la présence du plaignant au Canada ne sera pas préjudiciable à l'intérêt national, conformément au paragraphe 34(2) de la LIPR, ou qui puisse servir au plaignant, au besoin, pour demander une exception dite « exception ministérielle » à l'égard du paragraphe 34(2) de la LIPR.

Allegation de retard déraisonnable dans le traitement d'une autorisation d'accès à un site

Rapport n° 2007-06

Le CSARS a fait rapport d'une plainte présentée en vertu de l'article 41 de la *Loi sur le SCRS*, concernant le retard accusé par le Service à terminer son évaluation de sécurité aux fins de l'emploi du plaignant. Celui-ci avait reçu une offre d'emploi conditionnelle à l'obtention d'une cote de fiabilité et d'une autorisation d'accès à un site. Dans sa lettre d'offre, l'employeur précisait la date à laquelle le plaignant devait obtenir la cote et l'autorisation, faute de quoi il aurait le choix de prolonger le délai permettant de remplir la condition d'emploi ou d'annuler l'offre. Lorsque le CSARS a entamé l'audience de cette plainte, le SCRS n'avait pas terminé son évaluation de sécurité. Plus de 20 mois s'étaient écoulés depuis que le plaignant avait reçu l'offre d'emploi et il avait subi trois entrevues personnelles auprès du SCRS.

Le CSARS a conclu que, lorsque le plaignant a écrit au directeur du SCRS la première fois (environ deux mois après avoir reçu la lettre d'offre) pour se plaindre du temps pris par le SCRS pour terminer son évaluation de sécurité, la plainte était prématurée, en dépit de la date précisée par l'employeur dans l'offre d'emploi. Le CSARS a aussi conclu que, même s'il y avait un ensemble de retards mineurs, le temps global mis par le SCRS à terminer son évaluation de sécurité pendant les sept premiers mois était raisonnable. Cependant, le CSARS a établi que, après les sept premiers mois, même si les retards n'étaient pas délibérés, le temps mis par le SCRS à mener ses enquêtes de sécurité n'était pas raisonnable et les retards auraient pu être évités.

par la suite confirmé par le bref d'interdiction de territoire de 2004, et il a trouvé que les conseils du SCRS à CIC concernant cette affaire étaient appropriés.

Le CSARS a toutefois trouvé que d'autres aspects des conseils du SCRS à CIC étaient erronés ou inexacts, et donc non appropriés. Il n'a trouvé aucune preuve appuyant une croyance authentique que le plaignant ait été membre du MQM depuis son arrivée au Canada. Ce conseil était erroné et il a été perpétué dans le deuxième bref d'interdiction de territoire en 2004. Le CSARS a aussi trouvé une affirmation inexacte dans le bref d'interdiction de territoire de 2001.

De plus, le CSARS a examiné l'exception énoncée à la division 19(1)f)(iii)(B) de l'ancienne *Loi sur l'immigration*, selon laquelle un demandeur ne peut appartenir à la catégorie non admissible énoncée à l'alinéa f), ni être réputé interdit de territoire, s'il a convaincu le ministre de la Citoyenneté et de l'Immigration que son admission ne sera nullement préjudiciable à l'intérêt national. D'après une étude de l'évaluation de l'analyste du SCRS, l'analyste ne s'est pas occupé de l'exception.

Enfin, le bref d'interdiction de territoire de 2004 ne tenait pas compte du fait que la *Loi sur l'immigration* avait été remplacée par la *Loi sur l'immigration et la protection des réfugiés* et que l'exception énoncée à la division 19(1f)(iii)(B) de l'ancienne *Loi sur l'immigration* figure actuellement dans une exception générale, au paragraphe 34(2) de la LIPR. Il n'était donc pas approprié que le SCRS n'ait pas mis à jour son conseil en se reportant à la nouvelle loi. Le CSARS a trouvé que les conseils donnés dans le bref d'interdiction de territoire de 2004 étaient erronés du fait qu'ils n'appliquaient pas la nouvelle loi.

Le CSARS a aussi formulé deux constatations au sujet de la procédure.

La première constatation concernait la production de documents. À quatre reprises au cours de l'enquête, le CSARS a demandé copie des lignes directrices ou procédures pertinentes au filtrage de sécurité que le SCRS avait suivies pour fournir ses conseils à CIC. À la suite de l'audience, l'avocat du SCRS a remis au CSARS, selon l'engagement en ce sens, copie du Guide des procédures de filtrage de sécurité qui était en vigueur, à la connaissance du Service, au moment où il avait préparé le premier bref d'interdiction de territoire. Les procédures de filtrage de sécurité qui régissaient l'élaboration du deuxième bref d'interdiction de territoire en 2004 n'ont jamais été approuvées officiellement. Même si un témoin du SCRS a déclaré que toutes les procédures et lignes directrices avaient été respectées dans la préparation des brefs, le CSARS n'a guère pu tenir compte de ce témoignage, car le témoin n'avait personnellement pas pris part à leur préparation. De plus, le SCRS n'a pu dire au CSARS avec une entière certitude sur quels documents la préparation des brefs était fondée.

Le CSARS a en outre recommandé que le Ministre donne au plaignant la possibilité de faire une nouvelle demande d'habilitation de sécurité selon la nouvelle politique.

Enfin, le CSARS a recommandé que, si le plaignant faisait une nouvelle demande, le CSARS ou Transports Canada l'interviewe en présence d'un avocat ou d'un autre représentant. De plus, le plaignant devrait être informé de son droit d'enregistrer l'entrevue et le SCRS ou Transports Canada devrait aussi l'enregistrer et conserver copie de l'enregistrement jusqu'à ce que le plaignant ait eu l'occasion d'épuiser tous ses recours ou jusqu'à l'expiration de la période de conservation prévue dans la *Loi sur la protection des renseignements personnels*, en retenant la dernière échéance.

Présomption de mauvais conseils fournis au ministre de la Citoyenneté et de l'Immigration

Rapport n° 2007-05

Le CSARS a fait rapport d'une enquête qu'il a menée au sujet d'une plainte portée en vertu de l'article 41 de la *Loi sur le SCRS* et alléguant que le SCRS avait fourni de mauvais conseils à Citoyenneté et Immigration (CIC) en 2001 et en 2004 au sujet d'une demande de résidence permanente au Canada, présentée par le plaignant en vertu de l'ancienne *Loi sur l'immigration*.

Dans cette affaire, le plaignant était un réfugié du Pakistan. Dans ses documents d'immigration, il avait déclaré que, pendant qu'il était au Pakistan, de 1985 à 1996, année où il a immigré au Canada, il avait appartenu à l'organisation appelée Mouvement national unifié (Mutahida Qaumi Movement – MQM). En 2000, lorsque le SCRS l'a interviewé, il a fourni des détails sur son adhésion passée au MQM, disant à l'enquêteur qu'il n'avait rien eu à voir avec le MQM depuis sa venue au Canada.

À la suite de l'entrevue, le SCRS a présenté un « bref d'interdiction de territoire » à CIC en 2001. En 2004, il a mis à jour son bref à CIC. À l'époque du deuxième bref d'interdiction de territoire, la *Loi sur l'immigration* avait fait place à la *Loi sur l'immigration et la protection des réfugiés* (IPR) dont l'article 34 avait remplacé l'article 19 de l'ancienne loi.

L'enquête du CSARS visait en grande partie à déterminer si, de par la loi, le MQM est une organisation dont on a des motifs raisonnables de croire qu'elle se livre ou se livrait au terrorisme. Elle visait aussi à déterminer si les conseils du SCRS à CIC concernant cette affaire étaient appropriés. Le CSARS a reçu des éléments de preuve à la fois du Service et du plaignant concernant cette affaire. Il a examiné le libellé de la *Loi sur l'immigration* que le SCRS a appliquée dans le bref d'interdiction de territoire de 2001,

2. La décision du Ministre de ne pas accorder d'autorisation d'accès à un site, qui a empêché l'octroi du laissez-passer autorisant l'accès aux zones réglementées d'un aéroport, a été prise conformément au programme pertinent, et cela, pour des raisons de sécurité et non pour des motifs de distinction illicite fondés sur la race, sur l'origine nationale ou ethnique du plaignant ou sur sa religion.

3. Les évaluations de sécurité effectuées par le SCRS et par Transports Canada étaient viciées pour deux raisons :

- a) la procédure suivie par le comité d'examen et par le ministre des Transports en vertu du Programme est essentiellement injuste et viole les règles de justice naturelle, étant donné les conséquences graves de la décision du Ministre, soit la perte de son emploi par le plaignant;
- b) le SCRS ne s'est pas conformé en tous points à ses propres procédures.

Plus précisément, le CSARS a conclu que la procédure prévue selon le Programme est essentiellement injuste et viole les règles de justice naturelle en :

- ne fournissant pas au plaignant l'occasion de réfuter les renseignements défavorables avant que le Ministre prenne sa décision;
- n'exposant pas au plaignant les motifs de la décision du Ministre, ce qui lui aurait permis de faire un choix éclairé quant à la présentation d'une demande d'examen judiciaire;
- se fondant sur une évaluation de sécurité insatisfaisante;
- omettant de répondre en temps opportun aux demandes de renseignements téléphoniques de l'avocat du plaignant, ce qui, selon toute probabilité, aurait eu un impact sur la prise d'une décision éclairée, par le plaignant, de demander un examen judiciaire dans le délai de 30 jours.

Étant donné les conséquences graves de la décision du Ministre, qui ont entraîné la perte de son emploi par le plaignant, celui-ci aurait dû bénéficier d'un processus équitable, conforme aux règles de justice naturelle.

Le CSARS a recommandé que la Commission canadienne des droits de la personne ne fasse pas enquête sur cette plainte, conformément au paragraphe 46(2) de la *Loi canadienne sur les droits de la personne*. Il a soutenu que le Ministre n'avait pas pris la décision de refuser au plaignant une autorisation d'accès à un site en se fondant sur un motif de distinction illicite et que Transports Canada ne suivait pas une politique et/ou une pratique de refus d'autorisation d'accès aux personnes de même origine ethnique que le plaignant.

La pratique discriminatoire présumée concernait le fait que Transports Canada :

- n'avait pas délivré de laissez-passer autorisant l'accès du plaignant aux zones réglementées d'un aéroport, pour des motifs liés à la religion et à l'origine ethnique;
- avait adopté la politique et/ou pratique de refuser une habilitation de sécurité aux individus de même origine ethnique que le plaignant.

Selon le Programme d'autorisation d'accès aux zones réglementées d'aéroports (« le Programme ») de Transports Canada, le plaignant (qui travaillait pour un employeur du secteur privé) avait besoin d'une autorisation d'accès à un site pour obtenir un laissez-passer du Bureau de contrôle des laissez-passer dans les aéroports. Cela l'aurait assuré d'un accès aux zones réglementées d'un aéroport. L'objectif du Programme est de prévenir les actes d'interférence illicites avec l'aviation civile, et cela, par la délivrance d'une autorisation d'accès aux personnes qui répondent aux normes énoncées dans le Programme. L'objectif est de prévenir l'entrée non contrôlée, dans les zones réglementées d'aéroports inscrits sur la liste, d'une personne appartenant à l'une des catégories prévues de menaces à la sécurité.

Dans le cadre du processus de demande d'un laissez-passer par le plaignant, le directeur de la Sécurité préventive à Transports Canada a reçu, au sujet du plaignant, des informations découplant de vérifications de son casier judiciaire, de ses antécédents en matière de crédit et des fichiers du SCRS. Le directeur a décidé de convoquer un comité d'examen d'autorisation d'accès, qui a examiné les craintes que le SCRS lui avait communiquées en matière sécurité nationale et les résultats de la vérification du casier judiciaire. Le comité d'examen a décidé de recommander au ministre des Transports de refuser l'autorisation. Par la suite, le Ministre a refusé d'octroyer une autorisation d'accès à un site au plaignant. L'accès aux zones réglementées de l'aéroport en cause étant une condition d'emploi, l'intéressé a perdu son emploi.

Le ministre des Transports a pris la décision sans fournir au plaignant l'occasion « de connaître la teneur des objections [...] retenues contre lui » ou de réfuter les renseignements défavorables. On n'a pas, non plus, fourni de motif de refus au plaignant. Le Ministre l'a informé de l'existence d'un délai de 30 jours pour la présentation d'une demande d'examen de la décision par la Cour fédérale.

Le CSARS a formulé les constatations suivantes :

1. La plainte pour discrimination avait trait à une pratique mettant en cause la sécurité nationale et elle a donc été renvoyée à juste titre au CSARS en vertu du paragraphe 45(2) de la *Loi canadienne sur les droits de la personne*.

Selon la politique du SCRS, toute demande de ciblage doit tenir compte des antécédents, en matière de droits de la personne, d'un pays ou d'un organisme étranger dont l'information peut servir à étayer la demande.

En se fondant sur ces faits, le CSARS a conclu que le SCRS se soucie des droits de la personne, mais qu'il peut néanmoins utiliser des renseignements obtenus sous la torture. Même s'il n'a pas constaté d'« insouciance totale » à l'égard de preuves obtenues sous la torture, le CSARS a trouvé que le SCRS mettrait l'accent sur l'impact que la torture pouvait avoir sur la fiabilité de l'information utilisée dans l'exercice des responsabilités que lui confère la *Loi sur le SCRS*, plutôt que sur les obligations qui lui incombent à l'échelle nationale en vertu de la *Charte canadienne des droits et libertés* et du *Code criminel* du Canada et, à l'échelle internationale, selon les traités que le Canada a signés et qui rejettent totalement la torture.

Aux fins de cette enquête, le CSARS a trouvé que les constatations et recommandations du juge O'Connor, et toutes celles qui émaneront de l'enquête de l'honorable Jacobucci, feront en sorte que l'information obtenue dans le cadre d'échanges avec les organismes étrangers soit utilisée de manière à protéger les Canadiens des menaces à leur sécurité. Ces efforts respecteront aussi les valeurs de la société libre et démocratique du Canada, qui se traduisent dans la *Charte* et le *Code criminel*, et ses obligations issues de traités quant à l'horreur de la torture.

Le CSARS a recommandé que le SCRS mette en œuvre les recommandations formulées à son intention dans le rapport Arar. Une deuxième recommandation découlant de cette enquête ne peut être dévoilée pour des raisons de sécurité nationale.

Pratique discriminatoire présumée

Rapport n° 2007-04

Le CSARS a fait rapport d'une décision qu'il a rendue à l'égard d'une plainte en vertu de l'article 45 de la *Loi canadienne sur les droits de la personne*. Le plaignant a allégué avoir été victime de discrimination pour des motifs fondés sur la race, l'origine nationale ou ethnique et la religion, de la part de Transports Canada qui l'a traité de façon différente, à son détriment.

Le ministre des Transports a demandé à la Commission canadienne des droits de la personne de renvoyer l'affaire au CSARS.

Le CSARS a conclu que ce manque d'expertise a empêché le Service d'exercer une diligence raisonnable, non seulement pour évaluer la fiabilité de l'information, à savoir notamment si les renseignements avaient été obtenus sous la torture, mais aussi pour évaluer s'il y avait un risque crédible que l'échange d'information entraîne un recours à la torture ou y contribue.

Le CSARS a relevé les avis suivants fournis par le juge O'Connor dans son rapport :

« Les responsables canadiens doivent faire preuve de plus de raffinement dans leurs évaluations et tenir compte de toute l'information disponible afin de tirer des conclusions raisonnables quant à ce qui a pu se produire. Pour évaluer le risque de torture, la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants prévoit qu'il faut tenir compte des antécédents d'un pays en matière de droits de la personne. »

Au cours de son enquête, le CSARS a été informé que le SCRS avait du personnel compétent pour évaluer la fiabilité de l'information. Il n'a toutefois pas été informé, ni a-t-il pu déterminer, si le personnel du SCRS était compétent à faire des évaluations avisées quant à savoir si les échanges d'information risquaient de susciter une possibilité de complicité du Canada dans la torture ou d'y contribuer, ou encore d'occasionner d'autres transgressions des droits de la personne.

Dans son étude n° 2005-02 (CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post⁴), le CSARS avait constaté l'absence de tout document concernant les préoccupations possibles à l'égard des droits de la personne, évoquées par des entités telles que Amnesty Internationale et Human Rights Watch, à l'égard de la documentation d'une entente distincte et relativement nouvelle que le Service aurait conclue avec un certain service de renseignement. Le CSARS a constaté que cette absence de document ne respecterait pas la norme d'évaluation envisagée par le juge O'Connor pour assurer que le Canada ne soit pas complice de transgressions des droits de la personne.

Quant aux ententes conclues avec des pays ou organismes étrangers à l'égard de la collecte et du partage d'information et de renseignements, selon à la fois les instructions ministérielles et les politiques opérationnelles, le SCRS doit tenir compte des antécédents d'un pays en matière de droits de la personne. Cela comprend toute possibilité de transgression par les services de sécurité ou de renseignement. De plus, on envisagera de conclure des ententes avec des pays qui ne partagent pas le respect du Canada pour les droits démocratiques ou les droits de la personne seulement si ces rapports sont nécessaires pour sauvegarder la sécurité du Canada.

⁴ La liste complète des études du CSARS peut être consultée sur son site Web (www.sirc-csars.gc.ca).

Dans son enquête sur la plainte de M. Copeland, le CSARS avait accès à des renseignements classifiés qui étaient pertinents aux allégations, dont une version classifiée du rapport du juge O'Connor (le « rapport Arar »). Après avoir examiné tous les documents mis à sa disposition ainsi que les observations des parties, le CSARS n'a relevé aucune preuve d'« insouciance totale ».

Dans sa décision, le CSARS a noté que, le 29 juin 2005, le SCRS avait donné suite à deux recommandations pertinentes énoncées dans l'étude du CSARS sur le rôle joué par le SCRS dans l'affaire Maher Arar³. La première était que le SCRS modifie ses politiques opérationnelles de façon à devoir tenir compte des antécédents d'un pays ou organisme étranger en matière de droits de la personne au moment d'utiliser des renseignements reçus de ces sources dans une demande d'autorisation d'enquête. La deuxième recommandation était que le SCRS modifie la politique opérationnelle visant l'information contenue dans une proposition de voyage à l'étranger de façon à devoir tenir compte des antécédents des pays ou organismes étrangers en matière de droits de la personne, concernant les visites au Canada ou les voyages à l'étranger.

De plus, le CSARS a tenu compte de la recommandation 14, formulée par le juge O'Connor dans le rapport Arar :

« On ne devrait jamais communiquer d'information à un pays où il y a un risque crédible qu'elle entraînerait un recours à la torture ou y contribuerait. Les politiques devraient comprendre des directives visant expressément à éliminer toute possibilité de complicité du Canada dans la torture, à éviter le risque d'autres transgressions des droits de la personne et à assurer la responsabilisation. »

Le CSARS voit dans cette recommandation la norme que le SCRS devrait appliquer lors des échanges d'information. Comme le juge O'Connor l'a en outre affirmé :

« Au pays, la Charte canadienne des droits et libertés confirme le rejet total du recours à la torture. »

Même si le CSARS n'a relevé aucune preuve d'« insouciance totale » de la part du SCRS à l'égard des preuves obtenues sous la torture, il a constaté qu'au moment où la plainte a été déposée, le SCRS n'avait pas de politique visant expressément à éliminer toute possibilité de complicité du Canada dans la torture. Comme on peut le lire dans le rapport Arar, le SCRS n'avait aucun employé compétent à reconnaître les renseignements qui pouvaient avoir été obtenus sous la torture, mais « [l']évaluation du SCRS se concentre davantage sur la question de savoir si le Service est en mesure de corroborer l'information ».

³ La liste complète des études du CSARS peut être consultée sur son site Web (www.sirc-csars.gc.ca).

Comme pour toute autre plainte, la charge de la preuve incombe à la plaignante. Le CSARS a conclu que celle-ci n'avait pas présenté suffisamment de preuves pour établir la présomption d'intimidation et de mauvaise conduite.

Néanmoins, le CSARS a conclu que le conflit entre les deux parties aurait pu être évité si les politiques du SCRS avaient permis à l'intéressé qu'un avocat ou un autre représentant puisse non seulement assister à l'entrevue de filtrage de sécurité, mais aussi défendre cette personne pendant le processus d'entrevue avec le SCRS.

Le CSARS a recommandé que les politiques du Service soient modifiées de manière à permettre aux intéressés d'être accompagnés et pleinement représentés par un avocat ou par un autre représentant à une entrevue de filtrage de sécurité menée par le SCRS.

Présomption d'atteinte aux droits de la personne et de traitement injuste

Rapport n° 2007-02

Dans cette plainte présentée au CSARS en vertu de l'article de la 41 de la *Loi sur le SCRS*, le plaignant a allégué que le Service avait porté atteinte à ses droits individuels et à ceux de sa famille et qu'il l'avait traité injustement. Le CSARS a fait enquête sur la plainte et a conclu à l'absence de preuve d'atteinte aux droits de la personne, tel qu'il a été allégué. Il a trouvé que le plaignant avait bel et bien été traité injustement, mais dans une mesure beaucoup moindre que ce qui avait été allégué.

Allegations concernant l'utilisation par le SCRS de preuves obtenues sous la torture

Rapport n° 2007-03

Le CSARS a fait rapport d'une décision rendue à l'égard d'une plainte portée selon l'article 41 de la *Loi sur le SCRS*, dans laquelle le plaignant, Paul Copeland, a allégué une « insouciance totale » du SCRS à l'égard de preuves obtenues sous la torture.

Fait à noter dans cette affaire, dès que le CSARS eut entamé son enquête, le gouvernement du Canada a mis en œuvre une recommandation clé formulée par le juge O'Connor dans le rapport de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar. Le 12 décembre 2006, l'honorable Frank Iacobucci a été nommé pour enquêter sur les actions des responsables canadiens relativement à Abdullah Almaliki, Ahmad Abou-Elmaati et Muayyed Nureddin. En conséquence, le CSARS a décidé qu'il ne lui appartenait pas de formuler dans son rapport des constatations qui pourraient être l'objet de cette enquête.

C. Décisions du CSARS relatives aux plaintes 2007-2008

Présomption d'intimidation

Rapport n° 2007-01

Le CSARS a fait rapport d'une décision rendue en vertu de l'article 41 de la *Loi sur le SCRS* à l'égard d'une plainte concernant le comportement de trois agents du SCRS, de sexe masculin, pendant leur interaction avec la plaignante, une avocate. Celle-ci a allégué que les trois hommes s'étaient adressés à elle d'une manière physiquement menaçante et l'avait intimidée en présence de ses clients, à un bureau de Citoyenneté et Immigration Canada (CIC). Les clients de la plaignante, un mari et sa femme, avaient besoin d'une entrevue de filtrage de sécurité par le SCRS aux fins de leur demande de résidence permanente.

À l'insu de la plaignante, CIC avait prévu des entrevues séparées et simultanées pour chacun des clients par des agents du SCRS. Selon la plaignante, les deux entrevues étant ainsi fixées, elle ne pouvait y assister avec ses clients. Un conflit a surgi entre elle et les trois agents du SCRS quant au moment des entrevues et à son rôle pendant l'entrevue. La plaignante a dit s'être sentie menacée physiquement par les agents du SCRS et elle tremblait. Elle a aussi trouvé grossiers et sexistes leur comportement et leurs remarques. De plus, elle a allégué que les agents du SCRS étaient racistes.

Dans le cadre de l'enquête du CSARS, une audience a été tenue. La plaignante n'a pas cité de tiers indépendant à titre de témoin au sujet du prétendu comportement des agents du SCRS. Le CSARS a été mis en présence de deux interprétations, différentes mais également plausibles, du déroulement des événements.

Le CSARS a conclu que les trois agents du SCRS ont réagi d'une façon raisonnable en pareilles circonstances. Ils ont suivi la politique du SCRS concernant la conduite des entrevues de filtrage à l'immigration. Les trois agents ont soutenu que leur comportement ne visait pas à intimider, mais plutôt à déterminer quel était le problème au sujet des entrevues prévues. La perspective d'entrevues simultanées a suscité un conflit à la plaignante, tandis que celle de fixer à nouveau des entrevues consécutives en a suscité un au sein du SCRS.

Le CSARS a conclu que, compte tenu des circonstances de l'affaire, le conflit aurait mis les deux parties dans tous leurs états et leur comportement en aurait été modifié en conséquence. Néanmoins, le CSARS n'a trouvé aucune preuve que le comportement de la plaignante, dans son rôle d'avocat auprès de ses clients, ni celui des agents du SCRS ait été abusif, menaçant ou intimidant.

Détermination de la compétence du CSARS à examiner une plainte...

...en vertu de l'article 41

Selon l'article 41 de la Loi sur le SCRS, le CSARS est tenu de faire enquête sur les plaintes que « toute personne » peut porter contre « des activités du Service ». Pour qu'il fasse enquête, deux conditions doivent être remplies :

1. le plaignant doit d'abord avoir présenté sa plainte par écrit au directeur du SCRS sans recevoir de réponse dans un délai raisonnable (environ 30 jours) ou, s'il en a reçu une, sans que cette réponse le satisfasse;
 2. le Comité doit être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet ni entachée de mauvaise foi.
- Le CSARS ne peut enquêter sur une plainte qui peut être réglée autrement, par une procédure de griefs en vertu de la Loi sur le SCRS ou de la Loi sur les relations de travail dans la fonction publique.

...en vertu de l'article 42

Quant aux habilitations de sécurité, le CSARS est tenu, selon l'article 42 de la Loi sur le SCRS, d'enquêter sur les plaintes présentées par :

1. les personnes qui ne sont pas embauchées par le gouvernement fédéral à cause du refus d'une habilitation de sécurité;

2. les fonctionnaires fédéraux qui sont renvoyés, rétrogradés ou mutés ou qui se voient refuser une promotion ou une mutation pour la même raison;

3. les personnes qui se voient refuser un contrat de fourniture de biens ou de services au gouvernement, toujours pour le même motif.

Les plaintes de ce type doivent être présentées dans les 30 jours du refus d'une habilitation de sécurité. Le CSARS peut prolonger ce délai si on lui fait part de raisons valables.

Tableau 1
Règlement des plaintes

	2005-2006	2006-2007	2007-2008
Reportées de l'exercice précédent	18	24	20
Nouvelles	45	37	32
Total	63	61	52
Réglées	39	41	37
Reportées à l'exercice suivant	24	20	15
Rapports	4	5	6

L'équipe de juristes du Comité fournit des conseils sur la procédure et les questions de fond et contre-interroge les témoins du Service si ceux-ci doivent être entendus en l'absence du plaignant pour des raisons liées à la sécurité nationale.

FORMES DIVERSES DES PLAINTES

Les types de plaintes sur lesquelles le CSARS enquête sont décrits dans la *Loi sur le SCRS* et prennent diverses formes. En vertu de l'article 41 de cette loi, le CSARS peut enquêter sur n'importe quelles « activités du Service ». Selon l'article 42, il peut instruire les plaintes concernant le refus d'habilitations de sécurité à des fonctionnaires et à des fournisseurs de l'État. L'article 42 ne l'autorise pas à reconnaître sa compétence à instruire les plaintes concernant les contrôles d'antécédents ou les vérifications de fiabilité, à caractère moins intrusif, qui sont menés simplement pour déterminer la loyauté ou l'aptitude d'un fonctionnaire fédéral éventuel. C'est la procédure de grief prévue par l'organisme intéressé qui sert à régler ces plaintes.

Selon l'article 42 de la *Loi sur le SCRS*, les personnes qui se voient refuser une habilitation de sécurité doivent en être avisées par l'administrateur général de leur organisme. Elles ont le droit de porter plainte au CSARS qui, s'il y a lieu, fait enquête et présente ses constatations et recommandations au Ministre, au directeur du SCRS, à l'administrateur général concerné et au plaignant.

Si la Commission canadienne des droits de la personne reçoit d'un ministre un avis écrit concernant une plainte qui a trait à la sécurité du Canada, elle peut en saisir le CSARS. Sur réception d'un tel renvoi, le Comité fait enquête et lui présente ses constatations, ainsi qu'au directeur du SCRS, au ministre de la Sécurité publique, au ministre compétent et au plaignant. Il a aussi le pouvoir d'enquêter sur les affaires dont il est saisi en vertu de la *Loi sur la citoyenneté*.

Une fois son enquête terminée sur une plainte présentée en vertu de l'article 41, le CSARS remet un rapport de ses constatations et recommandations au directeur du SCRS, au ministre de la Sécurité publique et au plaignant². Les résumés de ces rapports, expurgés de manière à sauvegarder la sécurité nationale et la vie privée des intéressés, figurent également dans le rapport annuel du CSARS au Parlement.

Le tableau 1 fait état de toutes les plaintes qui ont été présentées au CSARS au cours des trois derniers exercices financiers, y compris celles qui lui ont été adressées à tort, qui ont été déclarées hors de sa compétence ou qui ont fait l'objet d'une enquête et d'un règlement sans audience (examen administratif).

² Le plaignant reçoit une version déclassifiée du rapport.

B. Enquêtes sur les plaintes

PROCÉDURE D'ENQUÊTE DU CSARS SUR LES PLAINTES

Outre sa fonction de surveillance, le Comité a charge d'enquêter sur les plaintes du public au sujet du SCRS. Sa tâche consiste à écouter les Canadiens et à leur répondre, car c'est là l'un des principaux rôles que lui a confiés le Parlement. Le CSARS étudie les plaintes portées par les citoyens concernant toute activité du SCRS, ou ayant trait au refus ou au retrait d'une habilitation de sécurité qui est nécessaire pour obtenir ou conserver un emploi ou un contrat auprès du gouvernement fédéral. La première étape de presque tout dossier de plainte est une demande de renseignements présentée au CSARS, à laquelle le personnel du Comité s'emploie à répondre rapidement. Il informe alors le plaignant éventuel des exigences de la *Loi sur le SCRS* pour que son affaire soit traitée à titre de plainte.

Lorsqu'il reçoit une plainte par écrit, le CSARS en fait un examen initial. Si elle ne répond pas à certaines exigences de la loi, il ne reconnaît pas sa compétence et n'enquête pas. S'il la reconnaît, le CSARS étudie la plainte à une audience quasi judiciaire présidée par un ou plusieurs de ses membres, secondés par le personnel.

Dans ses enquêtes sur les plaintes, le CSARS a tous les pouvoirs d'une cour supérieure et il a accès à toute information dont dispose le SCRS, sauf les documents confidentiels du Cabinet. Un plaignant a le droit d'être représenté par un avocat et de formuler des observations à l'audience. Une audience préliminaire peut être tenue pour arrêter une procédure, de concert avec le plaignant ou son avocat, ou avec les deux.

Types de plaintes

- Le CSARS peut faire enquête sur quatre types d'affaires :
- les plaintes du public « contre des activités du Service » (article 41);
 - celles concernant le refus d'habilitations de sécurité à des fonctionnaires et à des fournisseurs de l'État (article 42);
 - les allégations dont la Commission canadienne des droits de la personne saisit le CSARS;
 - les rapports du Ministre à l'égard de la *Loi sur la citoyenneté*.

Le CSARS a examiné l'enquête menée par le Service sur certains individus que l'on croit être des terroristes de deuxième génération ou des convertis de fraîche date aux interprétations extrémistes de l'islam. Il a aussi examiné l'exercice, par le SCRS, des pouvoirs reçus par la voie de mandats et l'utilisation qu'il fait des sources humaines.

Constatations

Le CSARS a conclu que, dans cette enquête, le Service s'est conformé à la *Loi sur le SCRS* ainsi qu'aux instructions ministérielles et aux politiques opérationnelles applicables. En particulier, il n'a relevé aucun sujet de préoccupation dans son examen des individus cibles, de l'élaboration et de l'exécution d'un mandat ainsi que de la gestion et de la direction de la plupart des sources humaines associées à cette enquête.

Quant à l'exploitation des sources humaines par le SCRS, le CSARS a noté que la direction du SCRS n'avait pas octroyé l'autorisation requise pour les opérations menées au sein d'institutions névralgiques, tel qu'il est prescrit par ses politiques sur les sources névralgiques¹. Ainsi, le CSARS a constaté qu'un enquêteur régional avait ordonné à une source humaine de recueillir de l'information au sein d'une institution névralgique sans d'abord obtenir l'approbation de la direction.

Le CSARS a aussi conclu que les documents liés à l'autorisation d'enquête ne donnaient pas un aperçu assez complet du problème, groupe, organisation ou individu cible, ou ne décrivait pas les activités de la cible proposée, tel qu'il est prescrit dans les politiques opérationnelles. En particulier, le CSARS estime que les documents auraient pu fournir plus de détails sur la manière dont l'enquête devait s'articuler autour des questions sources d'inquêtes nouvelles ou croissantes. Cette information manquant, l'enquête a servi de dossier opérationnel général pour l'enquête plus vaste sur l'extrémisme islamiste. Le CSARS croit que, si le SCRS avait clarifié et circonscrit l'enquête contextuelle, il aurait ainsi pu cerner plus efficacement les sujets de préoccupation grandissante et les isoler aux fins de l'analyse.

En conséquence, le Comité a recommandé que le SCRS définisse clairement cette enquête contextuelle au prochain renouvellement et qu'il détermine si elle doit porter sur les questions qui sont sources d'inquêtes croissantes.

¹ Les institutions névralgiques comprennent les secteurs universitaire, politique, médiatique, religieux et syndical.

Étude d'une enquête antiterroriste*

Étude n° 2006-08

* Note :

Cette étude n'était pas terminée au moment de mettre sous presse le rapport annuel de 2006-2007.

Contexte

Ces dernières années, les services de renseignement occidentaux ont relevé les activités de certains mouvements aux assises islamistes, dont les adeptes font usage de violence dans le monde entier contre « les ennemis déclarés de l'islam ». Au Canada, on nourrit des craintes de plus en plus vives face à l'émergence des menaces terroristes « locales » que posent les islamistes dits de deuxième génération, soit ceux qui sont nés ou ont grandi au Canada et qui embrassent par la suite des croyances radicales, de même que les convertis qui adhèrent aux interprétations extrémistes de l'islam. Le SCRS a qualifié d'importantes les menaces sous la mouvance d'Al-Qaïda, et notamment celles que présentent les individus qui, selon toute apparence, peuvent s'être fondus dans la société.

Le SCRS donne priorité à la détermination des facteurs qui peuvent pousser à la radicalisation afin de mieux comprendre pourquoi des individus qui naissent ou grandissent au Canada pourraient se tourner vers l'extrémisme, et de les empêcher de se livrer à des activités liées à la menace.

Le CSARS a tiré trois conclusions dont il a fait part au Service afin qu'il en tienne compte dans ses efforts pour faire face à ces priorités divergentes. Premièrement, le SCRS devra prendre conscience des problèmes constants de capacité des ressources humaines et s'y attaquer, surtout par rapport aux exigences d'une charge de travail accrue par suite de la transition d'agent de liaison-sécurité à agent à l'étranger. Les efforts pour relever ce défi dépendront de la mesure où le Service estimera nécessaire de soutenir la capacité de collecte de ce bureau. Deuxièmement, le CSARS a incité le Service à poursuivre ses efforts en vue d'intensifier ses rapports avec les organismes partenaires, stratégie qui saura contrebalancer la dépendance excessive face à des sources d'information particulières, de l'avis du CSARS. Troisièmement, celui-ci a encouragé le SCRS à continuer de peaufiner les plans et priorités qui sont axés sur les menaces émanant de l'extérieur du Canada. Compte tenu du fait que la réorganisation du Service est toujours en cours, cette étude n'a donné lieu à aucune recommandation.

Étude d'un bureau à l'étranger

Étude n° 2007-07

Contexte

Étant donné que la grande majorité des menaces auxquelles le SCRS doit faire face prend naissance outre-frontière, il a pris des mesures pour renforcer sa capacité de fonctionner efficacement à l'étranger. Depuis bien des années, le Service a des bureaux dans divers pays du monde. Leur nombre et leur emplacement sont classifiés, à l'exception des bureaux de Londres, Paris et Washington. Les représentants du SCRS qui y sont affectés, appelés agents à l'étranger, étaient autrefois des agents de liaison-sécurité (ALS).

L'étude d'un de ces bureaux à l'étranger, par le CSARS, visait à :

- examiner la nature et le volume des travaux liés à l'immigration dans ce bureau à l'étranger, et la mesure où les autres responsabilités (c.-à-d. la collecte de renseignements et la liaison) étaient équilibrées;
- étudier les relations du bureau avec les autres organismes canadiens présents dans le pays hôte;
- analyser les rapports de liaison du bureau avec les organismes étrangers pour assurer que le SCRS traitait avec prudence avec ces services de renseignements aux pratiques douteuses en matière de droits de la personne;
- s'enquérir des effets que la réorganisation opérée par le SCRS en 2006 a eus sur les travaux à ce bureau.

Constatations

L'examen mené par le CSARS dans ce bureau à l'étranger illustre les difficultés auxquelles se heurte le SCRS dans une région géopolitiquement complexe d'où proviennent des immigrants et qui est la source de menaces diverses. Le Service a des attentes élevées à l'égard des agents à l'étranger afin qu'ils répondent à ces demandes divergentes, ce qui requiert une bonne gestion du temps et une quête efficace de sources diverses d'information. Le CSARS a signalé la capacité de l'agent à l'étranger affecté à ce bureau de répondre à ces attentes divergentes.

Dans l'optique du CSARS, deux questions qui se chevauchent convergent à ce bureau : les défis de la restructuration stratégique et les attentes en matière de charge de travail tactique. Ces questions deviendront particulièrement pertinentes pour ce bureau à l'étranger, à mesure que la demande de renseignements de sécurité dans la région continuera d'évoluer. Pour le Service, le défi sera de savoir équilibrer l'accroissement de la demande de collecte et la réalité au niveau des ressources.

Pendant la période à l'étude, le CSARS a examiné la nature et l'ampleur des activités d'un échantillon de groupes et d'individus cibles, y compris ce qui faisait de ces cibles une menace pour la sécurité du Canada; il s'est en outre penché sur l'efficacité et la légitimité de l'enquête du Service.

Constatations

Cette étude a donné lieu à deux constatations et à une recommandation.

L'un des groupes examinés avait été approuvé à titre de cible en 2004 et à nouveau en 2006. Le CSARS a établi que le Service ne possédait aucun indice montrant que des membres du groupe cible avaient été mêlés directement à des actes liés au terrorisme. Selon le SCRS, sa préoccupation majeure était que des groupes terroristes puissent considérer ces individus comme des sujets de choix à recruter.

Malgré l'existence de preuves donnant à penser que ce groupe est une organisation terroriste – on croit, par exemple, que certains de ses membres ont pris part à des activités terroristes à l'extérieur du Canada – il existe aussi un vaste corpus de documents spécialisés qui donnent à penser que ce groupe est non violent et qu'il a été ciblé par divers gouvernements étrangers parce qu'il est considéré comme une menace politique. Le CSARS a noté dans son étude que, durant son enquête, le Service était au courant du débat concernant le statut du groupe à titre d'organisation terroriste, mais qu'il n'est pas fait allusion à ce débat dans le processus d'autorisation de l'enquête. En conséquence, la première constatation du CSARS est que ce processus aurait dû faire état de ce débat.

En conséquence, le CSARS a recommandé que le débat quant à savoir si le groupe cible est en fait une organisation terroriste devrait entrer dans les discussions futures sur le ciblage. Même si la discussion qui s'ensuivrait ne changerait peut-être pas la décision finale, le processus d'autorisation des enquêtes s'en trouverait néanmoins mieux éclairé.

Un autre volet de l'étude était l'examen de l'enquête menée par le Service sur des cibles au sein d'institutions névralgiques canadiennes, ce qui englobe les secteurs universitaire, politique, médiatique, religieux et syndical. Selon les instructions ministérielles et les politiques opérationnelles, le SCRS est tenu d'obtenir une autorisation d'un niveau supérieur avant d'entreprendre des activités d'enquête qui ont ou semblent avoir un impact sur ces institutions. La deuxième constatation du CSARS est que le SCRS peut devoir mener certains types d'activités d'enquête qui pourraient avoir un impact sur une institution d'un secteur névralgique. En conséquence, le CSARS estime que le Service devrait réexaminer ses politiques actuelles pour s'assurer qu'elles traitent comme il se doit de ces activités.

dans ce contexte sans cesse changeant, ce dont témoigne la création de la Région internationale et qui englobe la transition d'agent de liaison-sécurité à agent à l'étranger, et l'approbation de directives de la direction destinées à guider certaines opérations. Il reste toutefois du travail à faire.

En conséquence, le CSARS a formulé deux recommandations. Premièrement, son analyse donne à penser que le Service devrait repenser la structure de ses politiques afin de l'adapter à ses activités croissantes hors du Canada. Le Comité a constaté que le SCRS a revu ses pratiques afin de résoudre les difficultés cernées dans l'étude, mais qu'il n'a pas encore rajusté ses politiques correspondantes. Il estime qu'il y aurait lieu que le Service tire de ses pratiques actuelles des principes et thèmes communs afin d'élaborer une nouvelle politique destinée à guider les opérations faisant appel à des sources à l'étranger. Pour que ces changements soient efficaces, ils devraient être dirigés par le ministre de la Sécurité publique, au moyen d'une instruction ministérielle claire. En conséquence, le CSARS a recommandé que le SCRS priorise l'élaboration de ces politiques dès qu'il aura reçu la nouvelle instruction ministérielle.

La deuxième recommandation du CSARS concerne l'évaluation des risques des opérations faisant appel à des sources. Les documents de planification examinés qui font état d'évaluations de risques sont avarés de détails sur la manière dont ces évaluations ont été faites et manquent d'uniformité quant aux termes employés. En conséquence, il arrive souvent qu'on ne sait pas vraiment quels facteurs ont motivé l'évaluation d'un niveau de risque particulier. La politique du SCRS ne comporte ni échelle normalisée établissant les seuils des différents niveaux de risque, ni terminologie uniforme dans l'évaluation même de celui-ci.

Le CSARS a conclu que, dans ses plans d'ordre opérationnel, le SCRS devrait rationaliser ses procédures d'évaluation des risques et ses rapports sur les risques. Des normes claires fourniraient au personnel des opérations un outil calibré pour mesurer et évaluer les risques, et veiller à ce qu'on tienne compte de tous les facteurs. En conséquence, le CSARS a recommandé que le SCRS normalise ses évaluations de risques par une terminologie détaillée et uniforme qui se reflète dans ses politiques opérationnelles.

Étude d'une enquête antiterroriste

Étude n° 2007-06

Contexte

Cette étude a porté sur l'une des enquêtes les plus vastes et les plus hautement prioritaires du SCRS. L'activité opérationnelle liée à cette enquête s'est déroulée tant au Canada qu'à l'étranger, et le Service a coopéré avec des services de renseignement alliés afin de faire cesser certaines activités liées à la menace.

n'ont pas été communiqués efficacement, bien que rien ne prouve que cela ait affecté la qualité générale de l'opération. Le SCRS a informé le CSARS que, fort des leçons tirées à l'étranger, il avait recommandé des changements à apporter aux politiques existantes et que de nouvelles procédures sont constamment en voie d'élaboration et de mise en œuvre.

- L'opération a mis au jour les difficultés auxquelles le SCRS peut se heurter dans la conduite d'opérations faisant appel à des sources humaines à l'étranger. Le CSARS comprend qu'une évaluation de risques peut changer avec le temps et qu'une opération peut sembler plus ou moins risquée, avec du recul. Néanmoins, comme il est probable que le Service pourra continuer de prendre part au type d'opérations visées dans cette étude, soit des opérations faisant appel à des sources humaines, le CSARS lui a recommandé de revoir les critères guidant les évaluations de risques et de définir avec plus de précision les situations à niveau de risque élevé qui obligent à consulter le ministre de la Sécurité publique.

Étude des opérations du SCRS faisant appel à des sources humaines hors du Canada

Étude n° 2007-05

Contexte

La complexité des rapports avec les humains et des relations humaines en général fait des sources humaines un moyen unique et stimulant de recueillir des renseignements. Néanmoins, en matière de renseignement de sécurité, les sources humaines demeurent un moyen de compréhension essentiel tant du contexte de la menace que des intentions des cibles, ce qui n'est pas toujours évident à la lumière de sources techniques telles les photographies ou les communications interceptées.

Le CSARS a examiné les difficultés que présente la conduite à l'étranger d'opérations faisant appel à des sources humaines, y compris en zones de guerre. Il a évalué les actions du Service par rapport à la *Loi sur le SCRS* et aux instructions ministérielles, ainsi qu'aux politiques opérationnelles et aux lignes directrices pertinentes. Il s'est employé de façon spéciale à déterminer si les instructions ministérielles actuelles suffisaient à répondre aux activités du Service visant à recueillir des renseignements à l'étranger et à soutenir les opérations militaires.

Constatations

Le CSARS croit que l'expansion de son programme de collecte de renseignements étrangers sera une source de défis pour le SCRS en ce qui touche l'adaptation aux nouveaux contextes opérationnels. Il reconnaît les efforts du Service à travailler efficacement

groupes de pays étrangers; il en est de même des Canadiens qui travaillent ou se rendent à l'étranger. C'est ce qui a amené le directeur à affirmer qu'un des plus grands défis du SCRS est d'« augmenter [son] aptitude à mener efficacement à l'étranger des activités qui [l']aident à remplir [son] mandat de base en matière de sécurité nationale ».

L'étude du CSARS visait à examiner les efforts du Service pour accroître sa capacité à oeuvrer à l'extérieur du Canada. En conséquence, le CSARS a analysé, à titre d'étude de cas, le rôle du SCRS dans les efforts interministériels déployés à l'étranger pour venir en aide aux membres du groupe Christian Peacemakers, qui avaient été kidnappés en Iraq en 2005.

Voici les questions qui ont orienté les recherches du CSARS :

- Les instructions ministérielles existantes et les orientations fournies par les politiques sont-elles satisfaisantes compte tenu du caractère changeant des opérations du SCRS? Y a-t-il des leçons particulières que le SCRS peut tirer de sa participation aux initiatives interministérielles à l'étranger?
- À mesure qu'il étend sa capacité d'action à l'étranger, quelle est l'interaction du SCRS avec les ministères et organismes fédéraux qui ont aussi une présence internationale?

Constatations

Le CSARS a conclu que les agents du SCRS ont amélioré sur deux plans l'efficacité des efforts interministériels pour venir en aide aux membres kidnappés du groupe Christian Peacemakers. Premièrement, ils ont donné accès à l'information et aux priorités des autres services de renseignement oeuvrant en Iraq. Deuxièmement, les agents ont fourni des informations recueillies par les sources humaines à l'oeuvre dans la région.

Parallèlement, le CSARS a constaté que l'exemple des Christian Peacemakers illustrait les difficultés auxquelles le SCRS se heurtera en intensifiant ses activités à l'étranger :

- Il pourrait être nécessaire de mettre à jour les instructions ministérielles existantes pour fournir au SCRS des orientations appropriées.

- La soudaineté de la crise des Christian Peacemakers a fait ressortir l'importance de préparatifs matériels et logistiques et d'orientations quant aux politiques applicables. La Région internationale du SCRS a entrepris d'élaborer une infrastructure matérielle et stratégique pour répondre à de telles crises.

- L'opération de sauvetage a illustré la nécessité d'évaluations opérationnelles régulières, y compris des communications. Le CSARS a relevé deux cas où des renseignements

Premièrement, les récents changements organisationnels au sein de la DER devraient l'aider à améliorer sa capacité de production d'analyses de renseignements stratégiques et tactiques pour le gouvernement ou à l'appui des enquêtes du Service. En particulier, le CSARS estime que ces changements représentent une étape importante en vue de combler la nécessité d'analyses stratégiques à long terme plus nombreuses, en raison surtout du fait qu'il a mentionné dans de précédentes études que les nombreuses restrictions et l'insuffisance des ressources avaient limité la capacité du Service en matière d'évaluation du renseignement stratégique. Pour cette raison, le CSARS encourage la haute direction du SCRS à fournir le leadership et les ressources voulus afin d'assurer à la DER la stabilité organisationnelle nécessaire pour mener à terme ses initiatives et objectifs importants.

Deuxièmement, le CSARS croit que, dans l'ensemble de la collectivité du renseignement de sécurité, il y aura une demande accrue d'évaluations et de produits connexes de la DER. Pour le Service, et notamment pour la DER, le défi consistera à continuer d'accroître la capacité de répondre à ces besoins.

Troisièmement, le CSARS a constaté que la DER avait joué un rôle important et de plus en plus grand en collaborant avec d'autres éléments de l'appareil canadien du renseignement. Par exemple, les analystes de la DER entretiennent régulièrement des rapports avec l'ensemble de la collectivité du renseignement, sur un plan officiel, ces analystes et la haute direction participent à divers groupes de travail interministériels. Le CSARS croit que la participation courante de la Direction à ces initiatives est essentielle dans l'actuel contexte, complexe et changeant, qu'est celui de la sécurité.

Dans son étude, le CSARS a aussi fait ressortir diverses difficultés éprouvées par la DER à diffuser ses produits et à recueillir les réactions de ses clients. Il reconnaît les efforts du Service pour améliorer ses méthodes de liaison avec les clients de sorte qu'ils reçoivent en temps opportun des analyses et des commentaires pertinents.

Étude du soutien du SCRS aux opérations canadiennes à l'étranger

Étude n° 2007-04

Contexte

Dans son allocution prononcée en 2006 devant l'Association canadienne pour les études de renseignement et de sécurité, le directeur du SCRS affirmait que la frontière du Canada ne peut protéger le pays de nombreuses menaces qui pèsent actuellement sur celui-ci. La vie et les biens des Canadiens sont menacés par les actions d'individus et de

Le CSARS a recommandé que le SCRS consulte le Secrétaire du Conseil du Trésor en vue de clarifier sa responsabilité de faire enquête sur les incidents signalés selon la Politique du gouvernement sur la sécurité, et d'explorer l'utilité d'améliorer la liaison interministérielle afin d'informer les ministères de leurs responsabilités en matière de filtrage de sécurité selon la politique. Le CSARS encourage le SCRS à tenir compte de cette recommandation dans sa planification future et à l'inclure dans toute discussion avec le Secrétaire du Conseil du Trésor au sujet des responsabilités qui incombent au SCRS selon la Politique du gouvernement sur la sécurité.

Étude de la Direction de l'évaluation du renseignement du SCRS

Étude n° 2007-03

Contexte

La Direction de l'évaluation du renseignement (DER) (autrefois Recherche, Analyse et Production) du SCRS joue un rôle important pour ce qui est de fournir à point nommé des conseils stratégiques et tactiques au gouvernement fédéral concernant les menaces à la sécurité nationale. Pour le gouvernement ou à l'appui des enquêteurs du Service, la DER élabore des analyses stratégiques sur les tendances ou questions, actuelles et nouvelles, qui pourraient affecter la sécurité nationale dans l'avenir. Elle prépare aussi des analyses tactiques pour les besoins opérationnels, y compris de l'information sur certains individus, sur des cibles ou sur d'autres dossiers d'urgence immédiate.

Le CSARS a choisi d'étudier la DER afin de mieux comprendre la nature, l'étendue et l'efficacité de ses travaux. En plus de scruter les analyses de renseignements stratégiques et tactiques exécutées par la Direction, le CSARS a exploré la nature et l'ampleur de l'intégration et de la coopération de la DER avec la vaste collectivité canadienne du renseignement de sécurité et il a examiné comment elle avait diffusé en temps opportun des produits de renseignement pertinents.

Constatations

Dans l'ensemble, le CSARS a constaté que la DER est un groupe efficace, organisé de façon professionnelle, qui s'est employé avec diligence à répondre à une demande croissante d'évaluations et de produits de renseignements ces dernières années, à la fois au sein du Service et à l'échelle gouvernementale. Parallèlement, il lui reste encore beaucoup à faire pour s'adapter au contexte complexe et changeant du renseignement de sécurité. Cela, la direction de la DER l'a reconnu et l'a montré dans les travaux courants qui visaient à améliorer et à élargir le rôle de celle-ci. L'étude du CSARS a ouvert diverses perspectives sur la transition en cours.

de mettre au jour la relation des sources avec celui-ci. En conséquence, le CSARS a suggéré que le SCRS revise ses pratiques et mette en œuvre une approche uniforme à l'égard de toutes les opérations faisant appel à des sources humaines au Canada.

Enquête sur des préoccupations liées à la sécurité signalées selon la Politique du gouvernement sur la sécurité

Dans le cadre de cette étude, le CSARS a cerné et examiné le rôle joué par le SCRS dans l'enquête sur les préoccupations suscitées en matière de sécurité pendant la construction du complexe en surface du ministère de la Défense nationale à North Bay, en Ontario, dans le cadre du programme de modernisation du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD). Ces problèmes ont fait l'objet de deux rapports du Bureau du vérificateur général du Canada (mai et octobre 2007), mais aucun de ces rapports ne traite du rôle joué par le SCRS dans cette affaire.

Selon la Politique du gouvernement sur la sécurité, le ministère de la Défense nationale a charge de remplir ses obligations en matière de sécurité quant à la construction de ces installations et il doit signaler sur-le-champ au SCRS toute inquiétude qui surgit. De plus, le SCRS est l'organisme qui a charge d'enquêter sur les préoccupations signalées quant à la sécurité nationale. Dans cette affaire, le Ministère a fait état au SCRS des inquiétudes qu'il nourrissait en matière de sécurité et celui-ci a répondu en temps voulu. Le CSARS a toutefois noté que le SCRS n'avait pas obtenu, du ministère de la Défense nationale, une information suffisante pour qu'il puisse mener une enquête complète et proactive sur diverses inquiétudes touchant la sécurité des installations du NORAD.

Le CSARS a aussi décelé une lacune dans la politique canadienne sur la sécurité nationale. Selon la Politique du gouvernement sur la sécurité, tous les ministères sont tenus d'obtenir du SCRS des habilitations de sécurité pour les personnes qui doivent avoir accès à des installations protégées. Selon les deux rapports publiés par le vérificateur général en 2007, il arrive souvent que les ministères et organismes n'obtiennent pas les évaluations de sécurité requises pour les entrepreneurs. Pourtant, aucun mécanisme ne permet d'alerter le SCRS si un ministère ou un organisme ne respecte pas ces exigences.

Le CSARS croit que, si un ministère n'obtient pas les habilitations de sécurité requises, cela pourrait susciter une situation qu'un service de renseignement étranger pourrait exploiter. En conséquence, il a suggéré que le SCRS mette tout en œuvre pour être au courant des projets de construction comportant des installations protégées et pour élaborer une procédure normalisée lui permettant d'informer les ministères de la nécessité d'autorisations d'accès au site ou d'habilitations de sécurité.

Étude d'une enquête de contre-espionnage

En second lieu, selon l'alinéa 17(1)b) de la *Loi sur le SCRS*, le Service peut, avec l'approbation du Ministre, « conclure des ententes ou, d'une façon générale, coopérer » avec des services de sécurité ou de renseignement étrangers, ce que représentent les instructions ministérielles et les politiques opérationnelles. Dans son étude, le CSARS a trouvé des documents indiquant que le Service coopérait avec un organisme étranger avec lequel il n'avait pas conclu d'entente en vertu de l'article 17. Le SCRS a soutenu que les renseignements échangés avec cet organisme étaient visés par les ententes conclues avec d'autres organismes du pays en cause. Néanmoins, le CSARS a recommandé que le SCRS conclue une entente distincte en vertu de l'article 17 avec cet organisme afin de se conformer à la *Loi sur le SCRS*, aux instructions ministérielles et aux politiques opérationnelles.

Contexte

Dans cette étude, le CSARS a examiné l'une des enquêtes de contre-espionnage du SCRS les plus hautement prioritaires. Le service de renseignement étranger en cause a mené des opérations offensives au Canada, ciblant l'information économique, politique, scientifique et technique. Certaines de ses opérations avaient aussi visé des bureaux diplomatiques et du personnel canadiens oeuvrant à l'étranger.

L'étude du CSARS visait à évaluer le rendement du Service à parer aux tentatives de ce service de renseignement étranger pour cultiver des sources d'information au sein du gouvernement du Canada et pour se procurer clandestinement, auprès d'entreprises canadiennes, des renseignements économiques et des technologies contrôlées.

Constatations

Le CSARS a conclu que l'enquête du SCRS avait été menée de façon professionnelle et dénotait à la fois une puissante planification opérationnelle et une longue expérience. Le Service a montré qu'il était bien placé pour cerner et parer les nouvelles menaces que présentait ce service de renseignement étranger. Le CSARS a noté que le SCRS avait repensé et réorienté depuis peu ses efforts de renseignement pour faire face à un changement découlé dans les pratiques du service étranger en question. Le Service doit continuer à modeler son enquête de manière à contrebalancer les difficultés cernées dans cette étude et à combler les lacunes actuelles en matière de renseignement.

Le CSARS a aussi relevé une application incohérente des procédures concernant des rencontres protégées avec des sources humaines et il a exprimé la crainte que certaines pratiques pouvaient menacer la sécurité des opérations du SCRS et accroître le risque

Étude de la coopération du SCRS avec les services de renseignement d'un pays étranger et de son enquête sur ceux-ci

Étude n° 2007-01

Contexte

Les enquêtes de contre-espionnage menées par le Service sont depuis toujours axées sur les pays qui agissent en secret au Canada. Dans le cas qui nous occupe, le SCRS a collaboré avec les services de renseignement d'un pays étranger et il a fait enquête sur leur compte. Le CSARS était intéressé à examiner les défis qu'a dû relever le SCRS dans la gestion de ces relations tout en essayant de prévenir des activités présumées menaçantes. Le CSARS a aussi examiné si les renseignements échangés avec les organismes étrangers en cause et la coopération avec eux entraient dans le champ des ententes conclues avec ces organismes et si cette situation suscitait des problèmes ou des questions.

Constatations

Le CSARS a constaté qu'en dépit d'une coopération accrue entre le SCRS et les organismes cibles, il était tout à fait légitime que le Service enquête sur leurs activités clandestines. En pareilles circonstances, toute relation risquant de dégénérer en conflit, mais le CSARS a établi que le SCRS avait mené son enquête efficacement. Du même coup, il a confirmé que le Service devait demeurer prudent et maintenir un juste équilibre afin d'entretenir cette relation de manière à assurer la protection des intérêts du Canada en matière de sécurité. Le CSARS a aussi constaté que les employés du SCRS ne présentaient pas toujours le formulaire qu'ils sont tenus de remplir, selon les politiques opérationnelles, après s'être mis en rapport avec un représentant d'organisme étranger.

Le CSARS a formulé deux recommandations découlant de cette étude.

En premier lieu, le CSARS a recommandé que les employés du SCRS établissent par écrit un relevé standard des renseignements non opérationnels échangés avec des organismes étrangers. Ce relevé serait versé à la fois dans le dossier pertinent de « coopération avec » l'organisme en cause et dans la base de données opérationnelles. Il devrait aussi comporter des renvois aux renseignements opérationnels échangés avec ces organismes. Le CSARS estime qu'en raison de la multiplication des visites de représentants d'organismes étrangers, il importe de tenir les employés du SCRS au courant des renseignements échangés avec ces organismes de sorte qu'ils puissent avoir rapidement un aperçu global de ces interactions.

Le programme de recherche du CSARS est conçu de manière à englober un vaste éventail de sujets. Lorsqu'il décide des études à mener, le Comité tient compte des éléments suivants :

- les événements susceptibles de représenter des menaces à la sécurité du Canada;
- les activités particulières du SCRS qui pourraient porter atteinte aux droits et libertés individuels;

- le rapport annuel classifié que le directeur du SCRS présente au Ministre;
- la nécessité d'évaluer régulièrement chacune des directions opérationnelles du Service et chacun de ses bureaux régionaux;

- les pouvoirs que lui confère la *Loi sur le SCRS*, selon les détails qu'on y trouve;
- les priorités et préoccupations qui sont énoncées par le Parlement ou dans les médias;
- les engagements du CSARS à réexaminer des questions particulières;
- les questions cernées par le Comité dans l'exercice de ses fonctions relatives aux plaintes;
- les orientations stratégiques ou initiatives nouvelles annoncées par le SCRS ou par le gouvernement du Canada.

Cette approche permet au Comité de gérer le risque que comporte le fait de ne pouvoir examiner qu'un petit nombre des activités du SCRS une année donnée. Chaque étude est un « instantané » des actions du Service dans un contexte particulier. Depuis plus de deux décennies, les études du CSARS fournissent au Parlement et aux Canadiens un tableau complet des activités opérationnelles du Service et l'assurance que celui-ci exerce ses fonctions de façon judicieuse et efficace et dans le respect de la loi.

Pour chaque étude, les chercheurs du CSARS consultent de nombreuses sources d'information afin d'examiner des aspects particuliers des travaux du Service. Par exemple, en plus de consulter la documentation spécialisée et de mener des séances d'information avec des employés du SCRS, les chercheurs passent beaucoup de temps à lire divers documents à l'administration centrale du SCRS. Ce processus les amène à examiner les dossiers d'enquête sur des individus et des groupes, les dossiers de sources humaines, les messages opérationnels et d'autres communications pertinentes, les documents ayant trait à la coopération entre le SCRS et les organismes et partenaires étrangers et canadiens, les évaluations du renseignement et les documents ayant trait aux mandats, entre autres sources, qui varient selon les études. L'idée est de créer un corpus d'informations diverses qui permette au CSARS de veiller à examiner et à comprendre à fond les dossiers en cause. Le CSARS est heureux que le SCRS ait tout mis en œuvre pour lui faciliter et améliorer l'accès à ces sources d'information et il le remercie de ses efforts en ce sens.

Le Comité n'est qu'un des divers mécanismes qui sont conçus pour assurer la reddition de comptes du SCRS. Celui-ci doit en outre faire rapport de ses opérations par l'entremise de l'appareil gouvernemental en place, notamment le ministre de la Sécurité publique, l'inspecteur général du SCRS, les organismes centraux et le vérificateur général ainsi que les commissaires à l'information et à la protection de la vie privée du Canada.

A. Examen des activités de renseignement de sécurité du SCRS

EXERCICE DE SA FONCTION DE SURVEILLANCE PAR LE CSARS

Le Comité de surveillance des activités de renseignement de sécurité (CSARS), qui a été créé en 1984, est le seul organisme qui ait pour mandat d'examiner, à titre indépendant, les activités du Service canadien du renseignement de sécurité (SCRS).

Le CSARS, qui a été créé en vertu de la *Loi sur le SCRS*, fournit au Parlement, et par son entremise aux Canadiens, l'assurance que le SCRS exerce ses fonctions de façon judiciaire et efficace et dans le respect de la loi, des politiques et des instructions ministérielles. Ce faisant, le CSARS s'emploie à veiller à ce que le SCRS protège et respecte les droits fondamentaux et les libertés des Canadiens et

des Canadiennes.

Pour remplir son mandat, le Comité confie chaque année à son personnel diverses études qui fournissent un examen rétrospectif et une évaluation d'enquêtes et de fonctions particulières du SCRS. La *Loi sur le SCRS* lui confère des pouvoirs quasi illimités pour ce qui est de scruter le rendement du Service. Exception faite des seuls renseignements confidentiels du Cabinet, le CSARS a le pouvoir absolu d'examiner toute information qui relève du SCRS, quel qu'en soit le niveau de classification.

Les rapports d'étude du Comité contiennent des constatations et, s'il y a lieu, des recommandations. Une fois terminés, ils sont présentés à la fois au directeur et à l'inspecteur général du Service. En outre, en vertu de l'article 54 de la *Loi sur le SCRS*,

le CSARS est autorisé à présenter au ministre de la Sécurité publique un rapport spécial sur toute question que ses membres estiment revêtir une importance particulière, ou tout rapport spécial que peut lui demander le Ministre.

En quoi un organisme de contrôle diffère-t-il d'un organisme de surveillance?

Un organisme de contrôle suit en permanence ce qui se passe au sein d'un service de renseignement et il a pour mandat d'évaluer et de guider les enquêtes ou les travaux en cours « en temps réel ». Le CSARS est un organisme de surveillance de sorte qu'il peut, contrairement à un organe de contrôle, évaluer pleinement le rendement passé du SCRS sans être mêlé d'aucune manière à ses décisions et activités courantes d'ordre opérationnel.

Bilan de l'exercice 2007-2008

Section 1

Cela signifie que le CSARS doit parfois être critique face au rendement du SCRS, mais aussi qu'il applaudit, lorsque la chose est justifiée, à l'apport du Service à la sauvegarde de la sécurité du Canada. À tout moment, nous nous efforcerons de rester fidèles à notre engagement à gagner et à conserver la confiance de la population canadienne en nous acquittant du rôle que le Parlement nous a confié.

Agencement du rapport

Le rapport annuel du Comité de surveillance des activités de renseignement de sécurité compte trois sections.

Section 1 : Bilan de l'exercice 2007-2008

Cette section résume les études que le CSARS a effectuées et les rapports de plaintes qu'il a remis durant la période visée par le présent rapport.

Section 2 : Activités opérationnelles et mécanismes redditionnels du SCRS

Cette section expose les renseignements que le Service fournit au sujet de ses activités, plans et priorités opérationnels, et cela, par rapport à ses principales directions. Elle décrit aussi le cadre de politiques et de régie à l'intérieur duquel fonctionne le SCRS.

Section 3 : Au sujet du CSARS

Cette section fournit des détails sur les activités du Comité en matière de rayonnement, de liaison et d'administration, y compris sur son budget annuel et ses dépenses.

Nous espérons que les résumés déclassifiés des études et des décisions relatives aux plaintes, publiés dans nos rapports annuels, contribueront à éclairer le débat public constant quant au rôle du SCRS dans la protection de la sécurité nationale au Canada.

Dans le rapport annuel de cette année, le lecteur constatera que, dans deux décisions concernant des plaintes au cours de l'exercice 2007-2008, le CSARS a recommandé que le SCRS modifie sa politique prévoyant la destruction des notes opérationnelles, de manière à les conserver. Cette recommandation, qui reprend des recommandations antérieures, visait à assurer que les plaignants, et le CSARS en qualité d'organisme quasi judiciaire, aient pleinement accès à toute information ayant trait aux affaires dont le Comité est saisi et qu'il est appelé à trancher.

Nous sommes heureux que la décision rendue récemment par la Cour suprême du Canada dans l'affaire *Charakaoui c. Canada (Citoyenneté et Immigration)*, 2008 CSC 38, ait apporté des éclaircissemements sur cette question et qu'elle traduise des opinions souvent exprimées par le CSARS sur cette affaire. Étant donné que la *Charte canadienne des droits et libertés* entre en jeu plus souvent dans les affaires de sécurité nationale et par suite de la mise en place du processus des conseillers spéciaux, instauré depuis peu, les conseils des tribunaux sont à la fois importants et nécessaires si, en qualité de nation, nous voulons trouver et préserver un juste équilibre entre la sécurité nationale et les droits individuels.

Le CSARS cherche à donner un éclairage équitable et équilibré à ses examens du rendement du SCRS. Même si nous sommes conscients de la complexité croissante et des défis que comportent les travaux du SCRS, nous demeurons toujours attachés aux normes redditionnelles élevées qui sont essentielles à la légitimité d'un service de renseignement de sécurité au sein d'une société démocratique.

« Étant donné que la *Charte canadienne des droits et libertés* entre en jeu plus souvent dans les affaires de sécurité nationale et par suite de la mise en place du processus des conseillers spéciaux, instauré depuis peu, les conseils des tribunaux sont à la fois importants et nécessaires si, en qualité de nation, nous voulons trouver et préserver un juste équilibre entre la sécurité nationale et les droits individuels. »

Déclaration du Comité

Depuis plus de deux décennies, le Comité de surveillance des activités de renseignement de sécurité (CSARS) s'emploie à fournir au Parlement, et par son entremise aux Canadiens, l'assurance que le Service canadien du renseignement de sécurité (SCRS) exerce son mandat, qui est de sauvegarder la sécurité nationale de façon efficace et irréprochable. Ces dernières années, au milieu de changements radicaux à la nature et à la portée du paysage du renseignement de sécurité, la fonction redditionnelle du CSARS a acquis une importance croissante. Contrairement à la période de la guerre froide, marquée par une nette démarcation entre les intérêts de l'Occident et ceux des pays communistes, les menaces à la sécurité nationale sont aujourd'hui beaucoup plus diffusées et complexes, transcendant les limites politiques et géographiques et les frontières traditionnelles des pays. Les phénomènes du terrorisme transnational et du terrorisme d'origine intérieure sont deux exemples de cette évolution du contexte de la sécurité. Face à ce contexte qui évolue toujours, la plupart des pays occidentaux, dont le Canada, ont modifié de façon fondamentale leur approche des dossiers du terrorisme.

Cette transition a fait ressortir l'importance d'une surveillance indépendante, experte et informée du SCRS. Celui-ci a apporté de profonds ajustements à ses priorités et méthodes en matière de collecte de renseignements, que ce soit en réponse aux nouvelles mesures législatives, aux changements au processus d'attestation de danger pour la sécurité, à diverses décisions judiciaires, aux constatations découlant d'enquêtes publiques ou à une demande accrue d'évaluations du renseignement de sécurité de la part du gouvernement. Le CSARS s'est employé avec diligence à comprendre et à évaluer ces transformations, tout en veillant à ce que le SCRS agisse de façon irréprochable, efficace et conforme à la loi. Ses études et ses décisions relatives aux plaintes sont un important moyen de fournir aux Canadiens l'assurance que le SCRS continue d'enquêter sur les menaces nouvelles et changeantes à la sécurité nationale d'une manière qui respecte les principales valeurs démocratiques du Canada. Nous assumons cette responsabilité avec un profond sentiment de fierté et de probité.

Comme il a un accès presque illimité à toute information qui relève du SCRS, les documents confidentiels du Cabinet y étant l'unique exception, le CSARS jouit d'une situation unique pour situer le débat entourant la nature et la portée du contexte des menaces, et la manière d'y faire face. Le CSARS ne préconise aucun point de vue ni perspective stratégique particulière, mais ses études et ses décisions relatives aux plaintes fournissent d'importants instantanés des travaux du SCRS, permettant d'examiner la nature et l'ampleur du contexte des menaces et de déterminer si le Service répond à ces menaces de façon irréprochable et efficace et d'une manière conforme à ses pouvoirs et à ses autorisations.

Section 2 : Activités opérationnelles et mécanismes redditionnels du SCRS 33

A. Activités opérationnelles du SCRS 35

I. Renseignement 36

Direction du filtrage de sécurité 36

Direction de l'évaluation du renseignement 42

Direction des sources humaines et du soutien aux opérations 43

Direction des services techniques et scientifiques 43

Centre intégré d'évaluation des menaces 43

ii. Opérations 44

Mandats de la Cour fédérale : généralités et statistiques 45

B. Exigences en matière de rapports 46

Rapport annuel du directeur du SCRS (2006-2007) 46

Certificat de l'inspecteur général du SCRS (2006-2007) 47

Agissements illicites du SCRS 47

Communication d'informations 48

C. Ententes avec des organismes étrangers 49

Ententes avec des organismes canadiens 49

Ententes avec des organismes étrangers 50

D. Politiques et régie 51

Exigences nationales en matière de renseignement de sécurité 51

Instructions ministérielles 52

Politiques opérationnelles du SCRS 52

Règlements et nominations par le gouverneur en conseil 52

Section 3 : Au sujet du CSARS 53

Composition du Comité 55

Personnel et organisation 55

Activités du Comité 55

Budget et dépenses 56

Demandes en vertu des Lois sur l'accès à l'information et sur la protection des renseignements personnels 57

Résumé des recommandations du CSARS concernant les études 61

Résumé des recommandations du CSARS concernant les plaintes 63

Table des matières

Déclaration du Comité	v
Agencement du rapport	vii
Section 1 : Bilan de l'exercice 2007-2008	1

A. Examen des activités de renseignement de sécurité du SCRS	3
Etude n° 2007-01 – Etude de la coopération du SCRS avec les services de renseignement d'un pays étranger et de son enquête sur ceux-ci	5
Etude n° 2007-02 – Etude d'une enquête de contre-espionnage	6
Etude n° 2007-03 – Etude de la Direction de l'évaluation du renseignement du SCRS	8
Etude n° 2007-04 – Etude du soutien du SCRS aux opérations canadiennes à l'étranger	9
Etude n° 2007-05 – Etude des opérations du SCRS faisant appel à des sources humaines hors du Canada	11
Etude n° 2007-06 – Etude d'une enquête antiterroriste	12
Etude n° 2007-07 – Etude d'un bureau à l'étranger	14
Etude n° 2006-08 – Etude d'une enquête antiterroriste	15
B. Enquêtes sur les plaintes	17

C. Décisions du CSARS relatives aux plaintes 2007-2008	21
Rapport n° 2007-01 – Présomption d'intimidation	21
Rapport n° 2007-02 – Présomption d'atteinte aux droits de la personne et de traitement injuste	22
Rapport n° 2007-03 – Allégations concernant l'utilisation par le SCRS de preuves obtenues sous la torture	22
Rapport n° 2007-04 – Pratique discriminatoire présumée	25
Rapport n° 2007-05 – Présomption de mauvais conseils fournis au ministre de la Citoyenneté et de l'immigration	28
Rapport n° 2007-06 – Allégation de retard déraisonnable dans le traitement d'une autorisation d'accès à un site	30

Le 30 septembre 2008


L'honorable Stockwell Day, C.P., député
Ministre de la Sécurité publique
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Monsieur le Ministre,

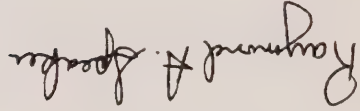
Tel qu'il est prescrit à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, nous vous présentons le rapport du Comité de surveillance des activités de renseignement de sécurité, pour l'exercice 2007-2008, afin qu'il soit transmis au Parlement.

Veuillez agréer, Monsieur le Ministre, l'expression de notre haute considération.

Le Président,



Gary Filmon, C.P., O.M.



Roy Romanow, C.P., O.C., c.r.



Raymond Speaker, C.P., O.C.

Les membres du CSAFS (de gauche à droite) :
l'honorable Baljit S. Chadha, l'honorable Gary Filmon (président), l'honorable Raymond Speaker,
l'honorable Aldea Landry et l'honorable Roy Romanow



Photo : Couvrette/Ottawa

Examen opérationnel du Service
canadien du renseignement de sécurité

Rapport annuel du CSARS 2007-2008



COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ



Comité de surveillance des activités de renseignement de sécurité

B.P. 2430, succursale D

Ottawa (Ontario)

K1P 5W5

(613) 990-8441

www.sirc-csars.gc.ca

Les appels à frais vîres sont acceptés de 8 h à 17 h, heure normale de l'Est.

Nota : Aux fins du présent document, la forme masculine désigne, s'il y a lieu, aussi bien les femmes que les hommes.

© Travaux publics et Services gouvernementaux Canada 2008

Nº de catalogue : PS105-2008

ISBN 978-0-662-05944-8



Examen opérationnel du Service
canadien du renseignement de sécurité

Rapport annuel du CSARS 2007-2008

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ





SECURITY INTELLIGENCE
REVIEW COMMITTEE

CA1
SIR
- A56



Annual Report 2008–2009

Accountability in a new era of
security intelligence

Security Intelligence Review Committee
P.O. Box 2430, Station D
Ottawa, ON K1P 5W5
(613) 990-8441

Visit us online at www.sirc-csars.gc.ca

Collect calls are accepted between 8:00 AM and 5:00 PM, EST

© Public Works and Government Services Canada 2009

Catalogue No. PS 105-2009

ISBN 978-1-100-50024-9



September 30, 2009

The Honourable Peter Van Loan, P.C., M.P.
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6



Dear Minister:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2008–2009, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

Gary Filmon, P.C., O.M.

Chair

Raymond Speaker, P.C., O.C.

Denis Losier, P.C.

Frances Lankin, P.C.

Arthur T. Porter, P.C., M.D.

WHAT IS SIRC?

The Security Intelligence Review Committee (SIRC, or the Committee) is an independent review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS, or the Service). By conducting reviews of CSIS activities and by investigating complaints, SIRC provides assurance to Parliament that the Service investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

WHAT IS CSIS?

CSIS is responsible for collecting and analyzing security intelligence and other related information within Canada and abroad. It advises the Government of Canada on issues and activities that are a threat to national security. CSIS also provides security assessments to all federal departments and agencies, with the exception of the Royal Canadian Mounted Police.

See Appendix B of this annual report for more information on some of CSIS's key activities.

CONTENTS

MESSAGE FROM THE COMMITTEE MEMBERS	2
ABOUT THIS REPORT	4
SECTION 1: THE YEAR IN REVIEW.....	5
SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS.....	8
A. REVIEWS.....	8
CSIS's Role in the Matter of Omar Khadr.....	9
CSIS's District Office Activities at Canadian International Airports....	13
A CSIS Human Source Operation	15
CSIS Activities at a Foreign Station	17
CSIS's Scientific and Technical Services	18
CSIS's Investigation into Domestic Extremism	19
The Case of Paul William Hampel	21
B. COMPLAINTS	22
Investigation of Alleged Profiling.....	24
SECTION 3: SIRC AT A GLANCE.....	26
Committee Activities.....	26
Committee Membership	26
Staffing and Organization	27
Budget and Expenditures.....	27
APPENDIX A: LIST OF RECOMMENDATIONS	28
APPENDIX B: CSIS AT A GLANCE.....	29
A. SECURITY INTELLIGENCE ACTIVITIES.....	29
Targeting	29
Warrants.....	30
B. SECURITY SCREENING ACTIVITIES.....	30
Government Screening	30
Site-Access Screening.....	32
Immigration Screening	33

MESSAGE FROM THE COMMITTEE MEMBERS

Security intelligence operates in an ever-changing environment. The nature and pace of that change today is on a scale that has not been seen for several decades in Canada and elsewhere. Faced with a diverse threat environment of state and non-state actors, increased foreign investigations, growing demands from government stakeholders, as well as numerous public inquiries and court decisions pertaining to national security, the world of security intelligence has become increasingly complex.

It is against this backdrop that the Security Intelligence Review Committee (SIRC, or the Committee) continues to serve Canadians to ensure the democratic accountability of one of our country's most secretive institutions. Our mandate remains firmly rooted in assuring Parliament that the Canadian Security Intelligence Service (CSIS, or the Service) investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians. However, the range of security intelligence-related issues that we must understand and review continues to evolve in nature and scope.

At SIRC, we take great pride in being an organization that makes full use of the range of tools at our disposal to fulfill our mandate. Through the *Canadian Security Intelligence Service Act (CSIS Act)*, Parliament gave this Committee a broad mandate to review the Service's performance in carrying out its duties and functions. Since it was first established in the 1980s, SIRC has endeavoured to fulfill this responsibility by responding to the changing priorities of CSIS and to the evolving expectations of Canadians for security intelligence in a democratic society. From the Committee's perspective, the *CSIS Act* has provided SIRC with a model framework to carry out its mandate.

Our annual report is a vital component of how we meet those expectations—maintaining a proud tradition of providing insight and analysis with probity and fairness. Given the nature and scope of the changes in the security intelligence environment, we feel this year is a fitting time to offer Canadians a new approach to the way we report our findings and recommendations.

This year's annual report includes an analysis section that identifies the main themes reviewed by SIRC in the past year and engages readers in a discussion about the importance of accountability in this new era of security intelligence. We are confident this undertaking will provide Parliament and all Canadians with a renewed understanding of SIRC's role in reviewing the operations of CSIS.

SIRC itself has also experienced important changes over the past year. We recently welcomed three new members to the Committee: the Honourable Frances Lankin, P.C., the Honourable Denis Losier, P.C., and the Honourable Dr. Arthur T. Porter, P.C., M.D. We all look forward to serving Canadians with the same level of commitment that has characterized SIRC's work since its inception. The Committee would also like to thank



Members of SIRC
(from left to right,
The Honourable
Raymond Speaker,
The Honourable Arthur
T. Porter, The Honourable
Gary Filmon (Chair),
The Honourable Frances
Lankin, The Honourable
Denis Loser.
Photo: Courlette Ottawa

those members whose terms ended recently: the Honourable Roy Romanow, P.C., O.C., Q.C., the Honourable Baljit S. Chadha, P.C., and the Honourable Aldéa Landry, P.C., C.M., Q.C. We thank them for their dedication and wish all of them well in their future endeavours.

On a final note, the Committee would like to take this opportunity to send our best wishes to Jim Judd, who, after serving as the Director of CSIS, retired from the public service in June 2009. From our perspective, Mr. Judd conscientiously guided the Service through some of the most challenging issues that the organization has faced in recent years. All Members of SIRC extend their thanks to Mr. Judd for his professionalism in meeting with the Committee on a number of occasions to discuss CSIS's work and the state of security intelligence. We look forward to working with his successor, Mr. Richard B. Fadden, and wish him well in his new position.

We are proud to share with Parliament and all Canadians our summaries of reviews and complaints investigations undertaken during the 2008–2009 fiscal year. It is our hope that this annual report will help inform Canadians about SIRC's roles and responsibilities and the constructive role we play in ensuring that CSIS is effective in investigating and reporting on threats to national security, while respecting the rights and freedoms of citizens. This is an integral part of the scheme of accountability that was established in 1984 by Parliament—a framework that has stood the test of time, and a responsibility that we look forward to continuing to fulfill with great pride.

ABOUT THIS REPORT

SIRC provides assurances to Parliament—and through it, to Canadians—that CSIS investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

The *CSIS Act* gives SIRC full access to any information under the control of the Service. As a result, SIRC may examine all of CSIS's files and all of its activities—no matter how highly classified that information may be. The sole exception is Cabinet confidences (e.g., written and oral communications that contribute to the collective decision-making of Ministers).

This annual report summarizes SIRC's key analyses, findings and recommendations arising from its reviews and complaints investigations. It has three sections:

SECTION 1: THE YEAR IN REVIEW

An analysis of prominent developments within the security intelligence milieu, and of how these relate to select findings and recommendations by SIRC from the past year.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

A synopsis of reviews completed by SIRC as well as the complaint reports it has issued during the period covered by this report.

SECTION 3: SIRC AT A GLANCE

Details about the outreach, liaison and administrative activities of SIRC, including its annual budget and expenditures.

A NEW LOOK FOR SIRC'S ANNUAL REPORT

As part of SIRC's ongoing efforts to understand and report on new challenges and responsibilities in security intelligence in Canada, a revised layout has been developed for the organization's annual report. Key elements of these changes include:

MORE IN-DEPTH

ANALYSIS FROM SIRC

The revised SIRC report explores the changing environment in which security intelligence operates. This includes observations about key trends and challenges that CSIS will need to address in the coming years.

EASY ACCESS

TO FACTS AND RECOMMENDATIONS

This report features a revised layout to help you find the facts and information you're looking for, including: recommendations made during the review period and important information on the Committee.

BACKGROUND

INFORMATION WHEN AND WHERE YOU WANT IT

Look for the caption boxes throughout this report. These contain valuable background information on various legal- and policy-related matters regarding SIRC's review and complaints functions.

SECTION 1: THE YEAR IN REVIEW

In less than two decades, the global environment in which Canada's security intelligence operates has undergone a fundamental transformation.

The end of the Cold War appeared to promise a more peaceful world with an expanding number of democracies and more widespread economic prosperity. It soon became clear, however, that the emerging global environment was both more complex and less secure than when there was a clear demarcation of interests between Western and Communist states.

The rise of global terrorism has played a significant role in shaping today's world, underscored most prominently by the rise of al Qaida as a globally capable terrorist platform. The 9/11 attacks on the United States, along with subsequent attacks in Europe and Asia, have changed how countries around the world perceive, and respond to, terrorism's destructive potential.

The contemporary threat environment is characterized by a constant danger of meticulously planned terror attacks designed to inflict mass casualties and destroy infrastructure. Canada has been openly threatened with attacks by al Qaida. It has also been subject to domestic and self-radicalizing terrorist cells. The arrest and trial of the Toronto 18 is reflective of this complex and evolving threat environment.

SIRC recognizes that CSIS must respond to these terrorist threats while still pursuing its traditional counter-intelligence priorities. For example, investigating the national security implications of the clandestine activities of foreign governments remains an important issue of concern. Likewise, counter-proliferation continues to be a top CSIS priority as the global community faces a number of unstable regimes with nuclear ambitions.

As the threat environment in which CSIS operates changes, so too does the corresponding legal environment. Recent court proceedings have lifted the veil of secrecy on the inner workings of the intelligence community. As part of this process, judicial rulings have required that the information CSIS brings to the courts meet the highest legal standards.

SIRC believes that the security intelligence environment will continue to be characterized by multiple threats and a high degree of unpredictability. Although global terrorism might shift its focus, it can be expected to continue to breed disorder and instability. Within this context, anticipating and defusing terrorist plans, while at the same time investigating other threats to national security, requires an effective security intelligence service.

When security agencies are faced with a multi-dimensional threat environment—and the need to protect society's fundamental values must be maintained—the role of a review body is equally complex. SIRC must comment on CSIS's capacity to carry out its mandate and on the tools that it has to undertake its work. Equally important, SIRC recommendations must be practical and reflect the values of Canadians.

SECTION 1: THE YEAR IN REVIEW

SIRC is the only independent review body with the mandate to comment on all aspects of the Service's operations. It can respond to complaints or, on its own initiative, review specific aspects of CSIS. It can also respond to requests from the Minister of Public Safety to review the Service's performance of its duties and functions.

Each year, SIRC reviews a selection of the Service's operational activities to determine if it acted appropriately, effectively and in accordance with the law. This year's annual report covers a range of CSIS's operational activities and deals with some of the complex issues that confront the Service. Section 2 of this report summarizes the Committee's reviews and complaint decisions.

In SIRC's view, CSIS has made important progress in developing policies to guide itself on human rights issues when investigating threats to national security. However, as SIRC's review of the Service's role in the matter of Omar Khadr reveals, there are additional issues to be addressed. Of particular note, CSIS must consider the principles of national and international law in regards to the treatment of minors when interviewing a Canadian detainee abroad.

Security agencies cannot investigate terrorist activities unless they exchange information efficiently across borders. Some of the countries that may possess vital intelligence on threats to Canada's security do not respect the human rights valued by Canadians. Canada does not use torture or approve of its use. Less straightforward, however, is whether CSIS should cooperate and interact with countries that may engage in human rights abuses to collect threat-related intelligence. As a result, it is increasingly important for SIRC to review the Service's interactions with foreign intelligence agencies.

A related issue arises if a CSIS representative interviews a Canadian detained abroad. The priority for CSIS is the collection of security intelligence. At the same time, it must consider suspicions of torture or other human rights abuses—whether a detainee is able to directly confirm them or not.

From SIRC's perspective, it is important for CSIS to address the many difficult issues that arise in conducting security intelligence work in a contemporary democracy. Most importantly, although intelligence collection is the Service's *raison d'être*, the Khadr review underscores how extra-intelligence matters must become an integral part of CSIS's decision-making processes. As part of this transition, CSIS must draw on the guidance of the Minister in addition to its own experience and resources.

In a separate review, the Committee examined CSIS's activities at Canadian airports. These locations can be targets for terrorist attacks because they concentrate large numbers of people and are a vital part of Canada's transportation infrastructure. CSIS activities at Canadian airports support the aviation security framework by providing national security advice and conducting interviews of persons suspected of posing a threat to national security. In reviewing the Service's activities at these airports, SIRC found that CSIS's presence enhances the security environment.

SIRC also examined the impact of legislation passed after 9/11 on CSIS's activities. For instance, one of the goals of the 2001 federal *Anti-Terrorism Act* (ATA, or the *Act*) was to address terrorism financing. However, the *Act* raised some difficult issues for CSIS in terms of managing its human source program. In particular, due to the ATA's provisions, activities related to CSIS's human source program that could benefit organizations listed as terrorist entities were, by definition, potentially criminal acts. Although CSIS has taken steps to address these issues, SIRC believes more accountability to the Minister of Public Safety is needed with respect to certain aspects of the Service's human source program.

SIRC's review of CSIS's investigation into domestic extremism found that key elements of the Service's strategy for dealing with the domestic threat environment needed to be reviewed and reformulated. The Committee believes this is necessary to ensure there is a clear and common understanding of both the threat environment and the terminology used to describe it. This task will become more pressing over the coming months in advance of the 2010 Olympic and Paralympic Winter Games in Vancouver—an event that will be a major test of Canada's security infrastructure.

SIRC has the power to comment on the manner in which CSIS has used its authorities, as well as whether those authorities are fair, reasonable and appropriate to the threat. The Committee's review of CSIS's Scientific and Technical Services commented on the continuing lack of lawful-access legislation and its impact on Service operations. This legislation is needed. It would require that Internet service providers include intercept capabilities in their networks. SIRC hopes that the government's latest legislative efforts on this matter are successful in achieving this goal.

The role of SIRC as a review agency would be straightforward if there were public successes and failures that could be analyzed for lessons learned. In the fortunate absence of an actual attack or a major security incident, SIRC examines aspects of CSIS operations, which can serve as valid indicators of the organization's capability, efficiency and effectiveness.

In the past, SIRC focused much of its review activity on CSIS operations within Canada. As CSIS moves to expand its capacity to operate outside of Canada, SIRC will accordingly allocate more of its resources to review these activities. As well, SIRC will continue to investigate complaints—not only to see if they are justified, but to determine whether they signal more systemic issues for review.

Because of its extensive powers to investigate CSIS, SIRC takes very seriously the duty to understand the complex challenges that CSIS confronts and to thoroughly review its activities.

SIRC's annual report is a vital component in meeting this expectation—one that has been entrusted to SIRC by Parliament, on behalf of Canadians.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

A. REVIEWS

For more than 25 years, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities. It has also scrutinized CSIS's performance of its duties and functions to determine if the Service acted appropriately, effectively and in accordance with the law.

SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and functions. The Committee's reviews include findings and—where appropriate—recommendations for the Service. Upon completion, all reviews are forwarded to both the Director of CSIS and the Inspector General of CSIS. SIRC is also authorized to provide special reports to the Minister of Public Safety on any matter that the Committee identifies as having special importance or that the Minister asks SIRC to undertake.

SIRC'S EARLIER REVIEWS

In past years, SIRC has reviewed a wide range of CSIS activities. For example, SIRC has examined how the Service carries out its mandate abroad by looking at activities undertaken at its various Stations around the world, the activities and investigations of CSIS regional offices, CSIS's cooperation and exchanges of information with domestic and foreign partners and specific operational activities such as CSIS's use of human sources. A complete listing of SIRC's past reviews can be found on the Committee's website (www.sirc-csars.gc.ca).

SIRC's research program is designed to address a broad range of subjects. In deciding which matters to review, SIRC considers:

- events with the potential to represent threats to the security of Canada;
- particular activities by CSIS that could have an impact on individual rights and freedoms;
- priorities and concerns identified by Parliament or in the media;
- issues identified in the course of SIRC's complaints functions;
- new directions or initiatives announced by, or affecting, CSIS;
- the CSIS Director's annual classified report submitted to the Minister of Public Safety; and
- the need to assess regularly each of the Service's branches and regional offices.

Each review results in a snapshot of the Service's actions in a particular context. This approach allows SIRC to manage the risk inherent in being able to review only a small number of CSIS activities in any given year.

SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work. As part of this process, researchers may arrange briefings with CSIS employees, as well as examine individual and group targeting files, human source files, intelligence assessments and warrant documents, plus files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources that vary between reviews. The goal is to create a diverse pool of information so that SIRC can ensure it has thoroughly reviewed and completely understood the issues at hand.

ACCOUNTABILITY MATTERS

SIRC is one of several mechanisms designed to ensure CSIS's accountability. In addition to the reviews and complaints investigations conducted by the Committee, the Service also remains accountable for its operations through the Minister of Public Safety, the courts, the Inspector General of CSIS, central agencies of government (e.g., Privy Council Office, Treasury Board Secretariat), the Auditor General, the Information Commissioner and the Privacy Commissioner of Canada.

SIRC Review: CSIS's Role in the Matter of Omar Khadr

CONTEXT

Many Canadians are familiar with the story of Omar Ahmed Khadr—a Canadian citizen held at the United States detention facility at Guantanamo Bay, accused of killing a United States army medic during a firefight in Afghanistan in 2002. The American legal case against Khadr, his treatment while in US custody, his status as a child soldier, and the Canadian government's stance on his repatriation—all of these topics have garnered widespread media coverage and commentary. In July 2008, Khadr's story was thrust onto the international stage when his lawyers released a videotape showing CSIS officials interviewing their client at Guantanamo Bay in February 2003. The video prompted questions in the public domain about the nature and extent of CSIS's involvement in this matter, including the reasons for the Service's decision to interview Khadr.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

SIRC'S LEGAL AUTHORITY IN THIS CASE

SIRC's review of CSIS's role in the matter of Omar Khadr was undertaken pursuant to Section 54 of the *CSIS Act*, which allows the Committee to forward to the Minister of Public Safety a special report on any matter that relates to CSIS's performance of its duties and functions. In most cases, these reports are reserved for matters that raise particularly difficult or high-profile issues that SIRC believes need to be brought to the Minister's direct attention. Examples of SIRC's previous Section 54 reviews include: the case of Mohammed Mansour Jabarah, the case of Maher Arar, the Heritage Front Affair, and CSIS activities in regard to the bombing of Air India Flight 182.

SIRC'S REVIEW

SIRC's objective was to conduct an in-depth review of CSIS's involvement in the case of Omar Khadr. The Committee looked back as far as mid-August 2002—when Canadian officials, including CSIS, were informed by American authorities that Khadr had been captured by US forces—to the federal court injunction in September 2005, prohibiting further interviews with Khadr by Canadian authorities.

In February and September 2003, CSIS officials travelled to Guantanamo Bay to meet with Khadr. SIRC noted that, from the Service's perspective, there were compelling operational reasons to interview him, given the threat posed by Sunni Islamic extremism in the months following 9/11. Khadr's father, Ahmed Khadr, was allegedly the highest-ranking Canadian al Qaida member. When the Americans granted Canadian intelligence and law enforcement officials access to Khadr, the Service seized the opportunity to gather intelligence that would advance their own investigation.

The driving force behind CSIS's interest in interviewing Khadr was to collect intelligence on a potentially serious terrorist threat and to provide advice to the Government of Canada accordingly. Although SIRC understands CSIS's position—that it had reasonable grounds to travel to Guantanamo Bay to gather threat-related information—the Committee found that the decision to interview Khadr was prompted primarily by intelligence considerations.

As a result, SIRC believes that CSIS failed to give proper attention to two important extra-intelligence matters: human rights issues and Khadr's age at the time that CSIS conducted its interview with him.

With respect to the first matter, SIRC examined the issues relating to the Service's handling of situations where it interacts and shares information with foreign partners when there are potential human rights considerations. CSIS's exchanges and cooperation with foreign

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

partners have come under closer scrutiny since 9/11, as it has become apparent that intelligence agencies need to work together to combat terrorist threats that transcend geo-political boundaries. Although information-sharing with foreign partners is crucial for CSIS to fulfill its mandate, it has created some new difficulties, specifically when working with countries that do not share Canada's respect for human rights.

The Canadian government fully supported CSIS's visit to, and interview of, Khadr at Guantanamo Bay in February 2003, as this initiative was part of a whole-of-government effort to gain access to him while in detention.

When CSIS interviewed Khadr in February 2003, there was widespread media reporting of alleged mistreatment and abuse of detainees in US custody in Afghanistan and at Guantanamo Bay. In mid-2002, allegations were made by several individuals relating to their treatment by American soldiers after being taken into custody in Afghanistan in late 2001 and 2002. Meanwhile, the US detention facility at Guantanamo Bay opened its door amid controversy as many countries denounced the American government's legal position, as well as its treatment of detainees.

SIRC did not find any evidence that CSIS took this into account in deciding to interview Khadr.

As a result of recommendations made by SIRC in 2004, and by Justice O'Connor in 2006 with respect to the case of Maher Arar, CSIS revised its policies governing the circumstances in which it shares information with foreign partners who are suspected of having questionable human rights records. CSIS and the Department of Foreign Affairs and International Trade (DFAIT) also signed a new protocol in 2007, to promote greater coordination and coherence across government in addressing issues that arise from consular cases involving Canadians detained abroad in cases related to suspected terrorism or national security. SIRC hopes that these developments will assist CSIS in the future in collecting intelligence while respecting human rights—particularly if confronted with situations similar to that of Khadr.

The second matter relates to Khadr's age. It is well recognized in Canadian and international law that youth are entitled to certain fundamental rights because of their status as a minor. In Canada, this is expressed in provisions of the federal *Youth Criminal Justice Act*. The rights of children are also reflected in international conventions to which Canada is party, such as the *UN Convention on the Rights of the Child*.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

NO EASY SOLUTIONS

The issues raised in this case—such as information-sharing with foreign partners, human rights concerns when dealing with youth, and interacting with detainees in foreign jurisdictions—do not present simple remedies or easy answers. New mechanisms have been established to encourage CSIS to consider such issues as part of its decision-making process. However, in SIRC's view, it is becoming apparent that finding a solution to many of these complex post-9/11 issues will entail a thorough rethinking of intelligence work in light of recent social, policy and legal decisions.

SIRC found no evidence that CSIS, in deciding to meet Khadr at Guantanamo Bay, took into account the fact that their interview subject was still a youth at the time. In addition, youth radicalization is of growing concern to the Service. In light of these facts, SIRC recommended that the Service consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.

Overall, SIRC believes that information-sharing with countries that have poor human rights records will continue to be a difficulty for CSIS until the Government of Canada resolves its seemingly contradictory position on information obtained from torture, versus the directions it provides to CSIS on carrying out its work.

This position places CSIS in an uncertain and vulnerable position when legal proceedings arise.

Such was the case in the matter of Omar Khadr, in which Canadian courts found that DFAIT and CSIS had violated Khadr's *Charter* rights by interviewing him and submitting the resulting information to US investigators. Underpinning the courts' message is that CSIS can no longer view the activities it undertakes strictly through the lens of intelligence-gathering. It must also consider the wider environment and implications within which its work is carried out.

There is general agreement among intelligence experts and academics that the world of intelligence changed dramatically after 9/11. Although CSIS has taken important steps to tackle some of these resulting challenges, the matter of Omar Khadr suggests that changes in policies and procedures are but one component of a broader transition that needs to take place.

The time may have come for CSIS to undertake a fundamental reassessment of how it carries out its work, and shift its operational culture to keep pace with the political and legal developments of recent years. It is also important for the Service to demonstrate that it has the professionalism, experience and know-how required to make the difficult

decisions that arise when conducting operations abroad. Indeed, there is mounting pressure and expectation on CSIS to consider extra-intelligence matters in fulfilling its mandate and carrying out its activities.

RECOMMENDATIONS IN BRIEF

This review had two recommendations:

- The Service should consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.
- CSIS should implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society. Guidance and advice from the Minister of Public Safety on how to accomplish this task would be helpful.

SIRC Review: CSIS's District Office Activities at Canadian International Airports

CONTEXT

A safe and secure civil aviation system is a vital component of Canada's economy. Its security is therefore of great importance. Following the 1985 bombing of Air India Flight 182 and the 9/11 terrorist attacks, a number of new measures were introduced across Canada to improve aviation security. These included new rules for aircraft and airport construction, enhanced screening of people and goods at airports, requirements for air carriers to provide basic information on specific passengers or flights, and assigning undercover police officers to provide security on Canadian aircraft. Although not an exhaustive list, these initiatives illustrate how civil aviation security has evolved into a broad network of players and responsibilities involving regional, provincial and federal agencies, as well as air carriers and private security firms.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

SIRC'S REVIEW

CSIS plays an essential role within the complex web of airport security stakeholders by investigating threats to national security, as well as screening passengers travelling to Canada or airport employees requiring access to restricted areas. In addition, CSIS activities at Canadian airports support the aviation security framework in their respective regions.

For this review, SIRC examined CSIS's activities at a selection of Canadian airports. The objective was to better understand and assess the role of CSIS at these airports, including how they manage their airport-related responsibilities and work with their airport partners.

Through constant contact with airport stakeholders, service personnel are able to transfer information to regions and headquarters, and act as conduits for information collection and sharing among airport partners. The effectiveness of their communications depends on maintaining solid relationships. SIRC observed that both of CSIS's District Offices spent considerable time and effort developing and maintaining contact with both government and non-governmental airport stakeholders.

Further, SIRC observed that government and law enforcement partners in the airport environment frequently request the assistance of CSIS personnel to obtain national security advice related to airport operations. CSIS airport personnel are called on by airport stakeholders to provide briefings on threat-related issues, including information concerning CSIS's national security mandate. Service personnel also provide advice to law enforcement agencies in response to any security breach or criminal incident occurring at an airport where a risk to national security is suspected. Airport immigration officers, as part of CSIS's role in the Port of Entry Interdiction Program, also request the presence of CSIS personnel when conducting interviews of air travellers who are suspected of posing a potential threat to national security. During these interviews CSIS personnel conduct background checks to determine if the person has a history of threat-related activities. This expert advice is vital in securing airport entry points.

CSIS staff also spend considerable time and effort building and maintaining relationships within the airport environment. Through the development of these relationships, CSIS airport personnel are able to support regional and headquarters operational desks that require access to the airport infrastructure to carry out operations.

SIRC noted that CSIS staff who carry out activities at airports would benefit from greater exchanges with their counterparts who serve airports in other regions of Canada, and who carry out day-to-day functions similar to their own. SIRC believes that Service personnel whose main functions are to support airport security should be given the opportunity to collaborate and share best practices with their counterparts at other airports.

Overall, SIRC found that CSIS activities at airports reinforce the Service's national security mandate. Moreover, this provides airport stakeholders with readily available access to CSIS expertise.

RECOMMENDATIONS IN BRIEF

There were two recommendations arising from this review:

- CSIS should support efforts that encourage greater collaboration between Service personnel to enhance their operational activities at Canadian airports.
- The Service should ensure that their disaster management plans include activities at airports, so that procedures are in place to better ensure that the essential services that they provide are not interrupted in the event that their offices are rendered inoperable.

SIRC Review: A CSIS Human Source Operation

CONTEXT

CSIS's human source program is considered to be an effective and cost-efficient intelligence tool. Sources under this program are often able to provide insight about a target's intentions—something that cannot be gained through the Service's other methods of information gathering.

Legislative steps taken to date to fight terrorism have presented the Service with unique challenges in terms of the management of the human source program. One such challenge arose as a result of the *Anti-Terrorism Act* (2001). Due to its provisions, activities related to CSIS's human source program that could benefit organizations listed as terrorist entities were, by definition, potentially criminal acts.

ABOUT THE *ANTI-TERRORISM ACT*

The *Anti-Terrorism Act* gives the Government of Canada legal authority to create a list of entities believed to be involved in terrorist activities. The *Act* also makes it a criminal offence to, among other things, directly or indirectly collect or make available property or financial or other related services knowing they will be used by—or will benefit—a terrorist group.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

Aware of the legal complexities of this situation, CSIS determined that its human source program was carried out within the confines of the law.

SIRC'S REVIEW

The Committee had briefly examined this issue in previous reviews. At that time, SIRC accepted the Service's position that CSIS operational policy was sufficient to cover all aspects of human source management. Nevertheless, SIRC maintained that it would continue to monitor the matter to identify challenging issues when required.

As part of this commitment, SIRC believed it was important to re-examine the matter at this time. For this review, SIRC placed special emphasis on the appropriateness and adequacy of the human source program's level of accountability within CSIS, and to the Minister of Public Safety.

In terms of accountability within CSIS, operational policy has not been updated to include any of the emerging factors that must be considered prior to determining whether actions carried out within the human source program are lawful. Nevertheless, SIRC found that a reporting structure was in place to ensure meaningful discussions take place within the Service about significant matters affecting management of the human source program.

In terms of accountability to the Minister of Public Safety, SIRC found that as a result of CSIS's interpretation—and by extension, its implementation—of operational policy, there was no venue by which it could inform the Minister of the implications of the *Anti-Terrorism Act* on human source operations. SIRC suggested a process of regularly updating the Minister on this matter.

Since the passage of the *Anti-Terrorism Act*, the Government of Canada has listed over 40 entities. As Canada's list of terrorist entities grows longer, commensurate growth is expected in the number of CSIS human source operations that could benefit listed organizations. It is important that CSIS be held to account for these activities.

RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should inform the Minister of Public Safety of the implications of the *Anti-Terrorism Act* as it relates to the Service's human source program and any future related developments.

SIRC Review: CSIS Activities at a Foreign Station

CONTEXT

In fulfilling its legal and operational responsibilities, CSIS maintains a presence outside of Canada. With the exception of three CSIS Stations—London, Paris and Washington—the locations are classified. Traditionally, the primary function of each Station was to liaise with CSIS's foreign partners and to conduct immigration screening. In addition, CSIS officials at headquarters used to manage operations abroad. Today, however, CSIS Stations take on larger roles in these operations. This expanded role coincides with an increase in the number of CSIS operations abroad, as underlined by former CSIS Director Jim Judd, who publicly acknowledged the Service's involvement in operations in Afghanistan, Iraq and Lebanon.

SIRC'S REVIEW

This year, the Committee examined the activities of a CSIS Station responsible for the Service's relationships with agencies in a number of countries. While not one of CSIS's busiest Stations, its work suggested that there was a high level of cooperation and information sharing. Although the Station under review was actively involved in operations, most continued to be managed by Canadian-based officials. Therefore, liaison work remained the Station's mainstay. Nevertheless, SIRC noted that the Station is well positioned to fulfill its mandate in liaison and operations.

To be effective in managing foreign relationships, all CSIS Stations need to have efficient methods of exchanging information—both with CSIS and its partner agencies. SIRC identified three communications-related challenges at the Station under review. In two instances, the challenges posed an inconvenience but did not prevent the Station from doing its work. SIRC also noted that CSIS had already indicated that it is exploring options to address these matters.

The third challenge related to the exchange of information directly from CSIS Headquarters to foreign agency representatives—as opposed to the accepted practice of sending the information through the respective CSIS Station. SIRC indicated that it would like to see a more consistent use of the accepted practice for exchanging information (i.e., all messages should go through the respective CSIS Station).

When the Service engages in operations abroad, senior-level approval is required from within CSIS. In recent years, this approval process was delegated downwards. The new process, however, was ambiguous and in some instances led to an inconsistent approach when seeking approval. New processes were recently instituted by CSIS, but these were outside of the scope of SIRC's work during the period under review. Nevertheless, it is worth noting that, in SIRC's estimation, the devolution of authority is a significant development that warrants ongoing examination.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

As CSIS Stations become more active operationally, they are addressing some of the needs that a separate foreign intelligence service would otherwise address. SIRC will continue to monitor the activities of both the Service and the Stations as they take on greater operational roles.

RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should ensure there is a more consistent use of the accepted practice for exchanging information with foreign partners in which all messages go through the appropriate CSIS Foreign Station.

SIRC Review: CSIS's Scientific and Technical Services

CONTEXT

Of all the strategies used by CSIS to collect and access information, those that are technology-based are considered to be the most resource-intensive. Designing and deploying these technologies requires a wide range of specialties including forensics, mechanical engineering, programming and laboratory analysis. These are all within the responsibilities of CSIS's Scientific and Technical Services (STS) Branch.

Although previous SIRC studies have examined aspects of the Service's technical operations, the Committee believed it was appropriate to conduct a more thorough analysis of what goes on behind the scenes within CSIS before an operation takes place.

SIRC'S REVIEW

The goal of this review was to better understand the nature and scope of the STS Branch's work, including the challenges it faces in completing its work and how it cooperates with various partners. Intelligence technology is a complex business that requires continued access to new talent and innovative research and development, as well as the ability to develop products in a timely fashion—all while dealing with budgetary constraints. The STS Branch manages these challenges by working with Government of Canada partners and contracting-out to industry.

During the review, it became apparent to SIRC that not all of the challenges STS faces are within its control to address. Primary among these is the need to keep pace with rapidly

developing technologies in a variety of disciplines. Associated with this is the absence of lawful-access legislation—requiring telecommunication service providers to design their products with built-in intercept capabilities. This is in sharp contrast to the experience of CSIS’s counterparts in the United States and Europe, where governments have legislated cooperation between the service providers and security intelligence agencies.

In Canada, opponents to lawful-access legislation cite a number of concerns, including:

- the appropriateness of compelling service providers to create intercept solutions;
- the scope of information that would be obtained and how it would be used; and
- whether restrictions or oversight would exist to prevent abuse.

Canada’s Privacy Commissioner has argued against various iterations of the proposed legislation, most recently stating that “lawful access raises fundamental issues for rights such as privacy and the ability to communicate freely.” The Committee recognizes it is important that Canadians engage in a healthy debate on this issue. However, SIRC is concerned that STS’s ability to perform certain investigative procedures will be constrained until the government is successful in enacting appropriate legislation.

On June 18, 2009, during preparation of SIRC’s 2008–2009 Annual Report, the federal government tabled the *Technical Assistance for Law Enforcement in the 21st Century Act*. If enacted, this legislation would require that internet service providers include intercept capabilities in their networks. SIRC will follow the development of this legislation to determine its potential impact on the Service’s intelligence-gathering mandate and priorities.

There were no recommendations arising from this review.

SIRC Review: CSIS’s Investigation into Domestic Extremism

CONTEXT

The Government of Canada considers domestic extremism a national intelligence priority. For this reason, CSIS identifies domestic, politically motivated violence as one of its highest priorities. The investigation of domestic extremism, however, presents a unique challenge to the Service. While it must gather information required to fulfil its mandate, CSIS must also refrain from infringing on Canadians’ protected rights to lawful advocacy, protest and dissent. Successfully negotiating the line between legal

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

protest and activist extremism requires a specialized and in-depth understanding of advocacy movements, protest tactics and the ways in which otherwise well-intentioned protesters can become radicalized.

SIRC'S REVIEW

This study had two objectives. First, SIRC examined CSIS activities in relation to domestic extremism, taking into account the overlap with criminal investigations and lawful advocacy, protest and dissent. SIRC found that CSIS had allocated appropriate resources to deal with the potential threat from domestic extremism. Moreover, CSIS had developed significant expertise regarding potential threats from domestic extremism, as well as a series of balanced measures to ensure Canadians' right to legal dissent.

However, SIRC found that some of the strategies employed by the Service to analyze the threat environment could benefit from reformulation. Several key concepts to evaluate the potential threat are not universally understood, commonly defined or used consistently. SIRC recommended that the Service establish an accepted terminology and gain a deeper understanding of the parameters of the threat environment to isolate and identify indicators of radicalization.

The second objective was to examine CSIS investigations of special events (i.e., an event that provides a heightened opportunity for carrying out threat-related activities). In that regard, the Committee examined the plans and priorities put in place by the Service for the 2010 Olympic and Paralympic Winter Games in Vancouver, and found them to be on-schedule and well-conceived. However, several of the concerns raised in the context of domestic extremism investigations—key concepts not being commonly defined or used consistently—applied equally to the Service's assessment of the threat environment surrounding the Olympic and Paralympic Games.

It is important to note that CSIS's understanding of the Olympics threat environment continues to evolve and its efficiency during the 2010 Games will depend on its ability to assess accurately the movements associated with domestic extremism. SIRC believes that the strategies recommended to address the concerns highlighted in the domestic extremism investigation will also inform CSIS's preparations for the Olympics.

RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should take steps to develop stronger definitions and a better understanding of the multi-issue extremism environment. The objective should be to build a more effective model to isolate and identify indicators of activist extremism and their potential for violence.

SIRC Review: The Case of Paul William Hampel

CONTEXT

Former CSIS Director Jim Judd has publicly acknowledged that foreign powers are becoming more sophisticated in conducting espionage within Canada's borders. A recent case of Russian espionage in Canada underlines this concern. In November 2006, a Russian spy, who had been using the name Paul William Hampel, was detained by Canadian officials in Montreal as he was about to board an international flight. The circumstances surrounding Hampel's detention received significant media attention, which reported that he was a Russian intelligence officer who had been residing in Canada under a false identity since 1995. However, there was no reporting of the nature and scope of CSIS's involvement in this high-profile and sensitive matter.

SIRC'S REVIEW

The objective of SIRC's review was to understand CSIS's involvement in the Hampel case. The Committee found that after becoming aware of Hampel's existence, CSIS conducted an investigation to determine the nature and scope of his espionage activities.

During the course of the investigation, the Service gathered important information to advise the Ministers of Public Safety and Citizenship and Immigration that Hampel was a known member of Russia's Foreign Intelligence Service and had used a fraudulent Canadian identity to further Russian espionage activities. In accordance with the *Immigration and Refugee Protection Act*, the Ministers signed a security certificate, thereby initiating the process by which Hampel was eventually deported to Russia.

As a result of the Hampel investigation, CSIS gained additional insights into the espionage threat posed to Canada by the activities of the Russian Intelligence Services. This will assist CSIS in investigating similar threats should they arise in the future.

There were no recommendations arising from this review.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

B. COMPLAINTS

In addition to its review function, SIRC is responsible for investigating complaints about CSIS. Almost all complaint cases begin as inquiries to SIRC—either in writing, in person or by phone. In turn, SIRC staff respond promptly, usually instructing the prospective complainant about what the *CSIS Act* requires for a concern to become a formal complaint.

WHAT IS THE DIFFERENCE BETWEEN A REVIEW AND A COMPLAINT INVESTIGATION?

A **review** is initiated by SIRC and entails in-depth research of CSIS's performance in carrying out its duties as described in the *CSIS Act*. A **complaint** investigation is initiated by an individual or group who may make a complaint to SIRC with respect to: "any act or thing done by the Service" (Section 41); denials or revocation of security clearances to government employees or contractors (Section 42); referrals from the Canadian Human Rights Commission; and Minister's reports in regards to the *Citizenship Act*. While reviews constitute SIRC's research function, complaint investigations are conducted as part of a quasi-judicial process.

Once a written complaint is received, SIRC conducts a preliminary review. Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated. If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee Members, assisted by staff. A complainant has the right to be represented by counsel and to make representations at the hearing. Pre-hearings may be conducted to establish and agree on procedures with the complainant and/or the complainant's counsel.

SIRC's legal team provides advice on procedural and substantive matters, and will also cross-examine Service witnesses when, for national security reasons, evidence must be heard without the complainant being present.

TYPES OF COMPLAINTS

The types of complaints that SIRC investigates are described in the *CSIS Act* and take several forms. Under Section 41 of the *CSIS Act*, SIRC can investigate "any act or thing done by the Service." Under Section 42, it can hear complaints about denials of security clearances to federal government

employees and contractors. Section 42 does not permit SIRC to accept jurisdiction to hear complaints concerning less intrusive background screening or reliability checks, which are conducted simply to determine the trustworthiness or suitability of a potential federal employee. These complaints are addressed through an organization's designated grievance procedure or potentially under Section 41 of the *CSIS Act*.

When SIRC's investigation of a complaint made under Section 41 is concluded, it provides a report to the Director of CSIS, the Minister of Public Safety and the complainant.¹ Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC's annual report to Parliament.

Pursuant to Section 42 of the *CSIS Act*, individuals who have been denied a security clearance must be informed of this action by the Deputy Head of the organization. These individuals have the right to make a complaint to SIRC and, where appropriate, SIRC will investigate and report its findings and any recommendations to the Minister, the Director of CSIS, the Deputy Head concerned and the complainant.

Should the Canadian Human Rights Commission receive a written notice from a Minister of the Crown about a complaint that relates to the security of Canada, the Commission may refer the matter to SIRC. Upon receipt of such a referral, SIRC carries out an investigation and reports its findings to the Commission, the Director of CSIS, the Minister of Public Safety, the Minister of the department concerned and the complainant. SIRC also has the authority to conduct investigations into matters referred to SIRC pursuant to the *Citizenship Act*.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC's jurisdiction, or investigated and resolved without a hearing (i.e., via an administrative review).

TABLE 1
RESOLUTION OF COMPLAINTS

	2006-07	2007-08	2008-09
Carried over	24	20	15
New	37	32	30
Total	61	52	45
Closed [†]	41	37	23
Carried forward to subsequent year	20	15	22
Reports issued	5	6	1

[†] Closed files include those where reports were issued, the Committee did not have jurisdiction, the preliminary conditions of the complaint were not met, or the complaints were withdrawn. In the past year, the Committee dealt with an increased number of files raising complex jurisdictional issues.

¹ The complainant receives a declassified version of the report.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

HOW SIRC DETERMINES JURISDICTION OF A COMPLAINT...

...UNDER SECTION 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by “any person” with respect to “any act or thing done by the Service.” Before SIRC investigates, two conditions must be met:

1. The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act*.

...UNDER SECTION 42

With respect to security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

1. Any person refused federal employment because of the denial of a security clearance;
2. Any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
3. Anyone refused a contract to supply goods or services to the government for the same reason.

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

SIRC Complaint: Investigation of Alleged Profiling

SIRC investigated a complaint in which the complainant was required to obtain an airport restricted-access security clearance for the purposes of employment. In this case, Transport Canada requested that CSIS undertake a security assessment to appraise this individual’s loyalty to Canada and reliability as it relates to such loyalty. The complainant was subsequently contacted by CSIS and a security-screening interview was conducted.

In the complaint to SIRC, filed pursuant to Section 41 of the *CSIS Act*, the complainant alleged profiling by CSIS. In addition, the complainant objected to the use of questions during the interview, which the complainant alleged solicited political opinions and were believed prohibited under the *Charter of Rights and Freedoms*. The complainant sought an apology and written assurances that CSIS would stop asking these questions at future security-screening interviews.

For its part, CSIS argued that it is not unusual to conduct interviews as part of the security screening process. Interviews may be conducted for cause when it is determined that there is insufficient information regarding an individual to complete a security assessment. In conducting its security assessment, CSIS is required, as per the *CSIS Act*, to appraise a person's "loyalty to Canada and reliability as it relates to such loyalty." In doing so, it will consider a range of factors when completing these assessments, including personal beliefs and associations—matters the Service considers to be consistent with the Treasury Board Secretariat's Government Security Policy.

SIRC's investigation included a detailed review of CSIS's documentation, as well as testimony from the complainant and representatives from CSIS plus a Treasury Board Secretariat representative who spoke about the purpose of the Government Security Policy. As a result of this information, SIRC was satisfied that CSIS acted in accordance with the Government Security Policy, the Government Security Policy Standard, as well as CSIS's applicable operational policies in requesting that the complainant attend a security-screening assessment interview. In addition, SIRC found that the complainant was not profiled on grounds prohibited by the *Charter of Rights and Freedoms*, and found that questions in the security-screening interview relating to the complainant's opinions and beliefs did not infringe on the complainant's rights under the *Charter*.

SIRC'S LEGAL AUTHORITY TO INVESTIGATE COMPLAINTS

Under Section 41 of the *CSIS Act*, SIRC has the authority to investigate complaints made by "any person" with respect to "any act or thing done by the Service." The Committee must also be satisfied that the complaint is not trivial, vexatious or made in bad faith.

ABOUT THE GOVERNMENT SECURITY POLICY

The Government of Canada must ensure that individuals who have access to government information and assets are reliable and trustworthy. Ensuring loyalty to Canada is essential for protecting Canadians and Canadian assets from threats posed by terrorism and espionage, or from malicious or improper activities, such as the unauthorized disclosure of classified and protected information that can have a serious impact on the safety of Canadians and on the effective functioning of society. Federal departments must therefore ensure that individuals are appropriately screened before commencing their duties. CSIS plays a vital role in this process, providing security assessments for government departments and institutions (see Appendix B of this report for further information on CSIS's security screening activities.) For more details on the Government Security Policy, visit the Treasury Board of Canada Secretariat's website (www.tbs-sct.gc.ca).

SECTION 3: SIRC AT A GLANCE

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Gary Filmon, P.C., O.M., who was appointed as Chair on June 24, 2005. The other Committee Members are the Honourable Frances Lankin, P.C., the Honourable Denis Losier, P.C., the Honourable Dr. Arthur T. Porter, P.C., M.D., and the Honourable Raymond Speaker, P.C., O.C.

All Members of SIRC are Privy Councillors. Each is appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the Opposition parties.

In addition to attending monthly committee meetings, members preside over complaints hearings, prepare reviews and complaint reports in consultation with SIRC staff, visit CSIS regional offices, address Parliamentary committees and exercise other duties associated with their responsibilities.

COMMITTEE ACTIVITIES

October 5–8, 2008: The Chair, the Executive Director, and a Member of SIRC attended the International Review Agencies Symposium, hosted in Auckland, New Zealand, by the Inspector-General Intelligence and Security.

October 30–November 1, 2008: The Executive Director and several staff attended a conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa.

November 4, 2008: At Carleton University, the Executive Director gave a lecture to students of a course on national security, providing an overview of SIRC's role and mandate.

March 5, 2009: The Executive Director appeared before the House of Commons Standing Committee on Public Safety and National Security.

March 24, 2009: The Acting Senior Counsel and the Senior Advisor met with officials from the New Zealand Security Intelligence Service.

March 26, 2009: The Acting Senior Counsel and the Senior Advisor met with officials from the Intelligence Security Committee (United Kingdom).

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 20, located in Ottawa. The staff comprises a Senior Advisor, a Senior Counsel, a Corporate Services Manager, Counsel, a Senior Paralegal, plus researchers and administrative staff.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

As part of their ongoing work, the Chair of SIRC, Committee Members and senior staff participate in regular discussions with CSIS executive and staff, and other senior members of the security intelligence community.

These exchanges are supplemented by discussions with academics, security and intelligence experts and other relevant organizations. These activities enrich SIRC's knowledge about issues and opinions affecting national security intelligence.

SIRC also visits CSIS regional offices on a rotating basis to better understand and examine the day-to-day work of investigators in the field. These visits give Committee Members an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. It is also an opportunity to communicate SIRC's focus and concerns.

During the 2008–09 fiscal year, SIRC visited three regional offices.

BUDGET AND EXPENDITURES

SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures. Table 2 below presents a breakdown of actual and estimated expenditures.

TABLE 2
SIRC EXPENDITURES 2008–09

	2008–09 (Estimates)	2008–09 (Actual)
Personnel	\$1,900,000	\$1,700,000
Goods and Services	\$1,000,000	\$700,000
Total	\$2,900,000	\$2,400,000

APPENDIX A: LIST OF RECOMMENDATIONS

During the 2008–2009 review period, SIRC made the following recommendations stemming from the range of reviews it conducted, as well as from the complaint it investigated.

CASE ²	SIRC RECOMMENDED THAT...
CSIS'S ROLE IN THE MATTER OF OMAR KHADR	<p>The Service should consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.</p> <p>CSIS should implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society. Guidance and advice from the Minister of Public Safety on how to accomplish this task would be helpful.</p>
CSIS ACTIVITIES AT CANADIAN INTERNATIONAL AIRPORTS	<p>CSIS should support efforts that encourage greater collaboration between Service personnel to enhance their operational activities at Canadian airports.</p> <p>The Service should ensure that their disaster management plans include activities at airports, so that procedures are in place to better ensure that the essential services that they provide are not interrupted in the event that their offices are rendered inoperable.</p>
A CSIS HUMAN SOURCE OPERATION	CSIS should inform the Minister of Public Safety of the implications of the <i>Anti-Terrorism Act</i> as it relates to the Service's human source program and any future related developments.
CSIS ACTIVITIES AT A FOREIGN STATION	CSIS should ensure there is a more consistent use of the accepted practice for exchanging information with foreign partners in which all messages go through the appropriate CSIS Foreign Station.
CSIS'S INVESTIGATION INTO DOMESTIC EXTREMISM	CSIS should take steps to develop stronger definitions and a better understanding of the multi-issue extremism environment. The objective should be to build a more effective model to isolate and identify indicators of activist extremism and their potential for violence.

² Consult the SIRC website at www.sirc-csars.gc.ca for a list of all SIRC reviews conducted since 1984.

APPENDIX B: CSIS AT A GLANCE

Each year, as part of SIRC's annual report, the Committee presents important information and statistics related to CSIS operations. This data, provided by the Service, provides readers with insight into some of the Service's key duties and functions, as well as highlights any major changes or developments within CSIS.

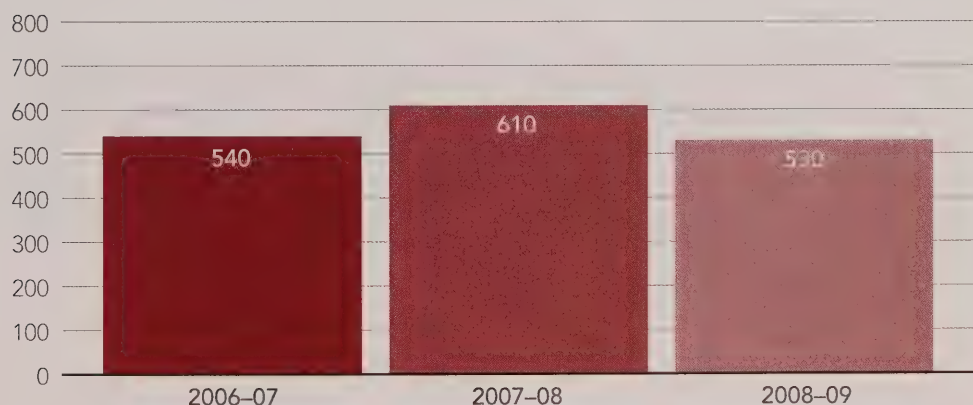
For SIRC's 2008–2009 Annual Report, this information is grouped in two categories: security intelligence activities and security screening activities.

A. SECURITY INTELLIGENCE ACTIVITIES

Targeting

When the Service has reasonable grounds to suspect that an individual or an organization could pose a threat to Canada, it must first establish an investigation in which it exercises its powers proportionate to the threat that is posed. Figure 1 indicates the number of targets investigated by CSIS during the period under review, relative to previous fiscal years.

FIGURE 1
TARGETING STATISTICS*



Note: * Figures have been rounded to the nearest 10.

Warrants

The power to authorize intrusive investigative techniques rests strictly with the Federal Court of Canada. If the Court grants a warrant, it provides CSIS with authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telecommunications activities. Table 3 shows the number of federal court-approved warrants that CSIS had during the period under review, relative to previous years.

TABLE 3 WARRANT STATISTICS			
	2006–07	2007–08	2008–09
New warrants	42	71	26
Replaced or renewed	134	182	183
Total	176 [†]	253 ^{††}	209 ^{†††}

[†] Included in this number were 25 urgent warrants

^{††} Included in this number were 19 urgent warrants

^{†††} Included in this number were 2 urgent warrants

B. SECURITY SCREENING ACTIVITIES

Security screening is one of the most publicly visible functions provided by CSIS. This activity consists of government screening (which includes site-access screening) and immigration screening.

Government screening

This type of screening provides security assessments—an appraisal of the loyalty to Canada and (so far as it relates thereto) the reliability of an individual—for all government departments and institutions, except the Royal Canadian Mounted Police (RCMP).

CSIS does not decide who receives a security clearance. Rather, it advises the requesting department or agency of information that could have an impact on their decision to grant a clearance. On rare occasions, CSIS will recommend to a requesting agency that the threshold in the Government Security Policy has been met to deny a clearance. However, it is the responsibility of the requesting agency to grant, revoke or deny a clearance.

Table 4 reports the number of requests for government screening that CSIS received over a three-year period. Table 5 reports the median turnaround time for CSIS to complete these assessments.

TABLE 4
REQUESTS FOR CSIS GOVERNMENT SECURITY SCREENING*

	2006-07	2007-08	2008-09
Requests from Department of National Defence (DND)	13,100	8,800	15,300
Requests from other clients	38,100	41,500	46,400
Total	51,200	50,300	61,700
Assessments issued to DND	13,100	8,300	14,400
Assessments issued to other clients†	41,800	40,500	46,300
Total	54,900	48,800	60,700

* Figures have been rounded to the nearest 100.

† This number includes assessments performed for provincial governments and for access to nuclear facilities.

TABLE 5
MEDIAN TURNAROUND TIME (IN CALENDAR DAYS)
FOR CSIS TO COMPLETE SECURITY ASSESSMENTS

		2006-07†	2007-08		2008-09	
			New	Updates	New	Updates
DND	Level I (Confidential)	40	23	9	74	57
	Level II (Secret)	40	28	23	61	62
	Level III (Top Secret)	82	164	29	126	57
Non-DND	Level I (Confidential)	32	18	13	18	6
	Level II (Secret)	21	13	12	15	16
	Level III (Top Secret)	47	186	4	145	8

† For 2006-07, median turnaround times for new and update security assessments were not available. The time reflected in this column is therefore for both types of assessments.

Site-access screening

This type of screening allows an individual access to certain secure areas—such as airports, port and marine facilities, the Parliamentary Precinct and nuclear power facilities—and provides accreditation for special events and assessments to provincial departments. These programs are meant to enhance security and reduce the potential threat from terrorist groups and foreign governments, which may seek to gain unauthorized access to classified information or other assets, materials and sensitive sites. Table 6 reports the number of requests that CSIS received for site-access screening over the past year, relative to the previous two years.

TABLE 6
REQUESTS TO CSIS FOR SITE-ACCESS SCREENING*

	2006–07	2007–08	2008–09
Parliamentary Precinct	1,100	1,100	1,000
Airport restricted-access area (Transport Canada)	39,300	36,800	31,400
Nuclear facilities	17,900	9,200	11,100
Free and Secure Trade (FAST)	23,100	10,700	6,400
Special events accreditation	0	1,300	16,300
Marine Transportation Security Clearance Program [†]	N/A	6,300	5,200
Other government departments	2,500	2,100	2,600
Total	83,900	67,500	74,000

* Figures have been rounded to the nearest 100.

[†] The Marine Transportation Security Clearance Program became operational in December 2007 to provide security assessments in relation to the security of Canada's ports

Immigration screening

This type of screening helps to ensure that individuals who pose a threat to security and/or are inadmissible under the *Immigration and Refugee Protection Act* do not gain entry or obtain status in Canada. If an individual meets one or more of these criteria, CSIS will issue a brief. Table 7 reports the number of citizenship and immigration screening requests received by CSIS, as well as the number of briefs issues in relation to these requests.

TABLE 7
REQUESTS TO CSIS FOR CITIZEN AND IMMIGRATION SCREENING
AND BRIEFS ISSUED

	Requests*			Briefs		
	2006-07	2007-08	2008-09	2006-07	2007-08	2008-09
Permanent resident [†]	62,800	66,000	67,300	201	195	213
Front-end screening ^{††}	17,900	21,800	26,800	143	117	108
Refugee determination ^{†††}	11,600	6,600	6,600	153	142	102
Subtotal	92,300	94,400	100,700	497	454	423
Citizenship applications	227,300	190,000	169,500	155	109	169
Total	319,600	284,400	270,200	652	563	592

* Figures have been rounded to the nearest 100.

[†] This includes permanent residents inside and outside Canada (excluding the Refugee Determination Program), permanent residents from within the United States and applicants from overseas.

^{††} Individuals claiming refugee status in Canada or at ports of entry.

^{†††} Refugees, as defined by the *IRPA*, who apply from within Canada for permanent resident status.

Table 8 reports the time it took for CSIS to complete notices of assessment, which are issued in those government and immigration screening cases when CSIS finds no adverse information on an applicant.

TABLE 8 TURNAROUND TIME (IN DAYS) FOR CSIS TO COMPLETE NOTICES OF ASSESSMENT			
	2006-07	2007-08	2008-09
Citizenship	1	1	1
Immigration (Canada) [†]	78	59	95
Immigration (USA) ^{††}	29	45	65
Overseas immigration	14	20	26
Refugee determination	98	64	89
Front-end screening	19	28	29

[†] This includes certain classes of individuals who apply for permanent resident status from within Canada.

^{††} This includes persons who have been legally admitted to Canada for at least one year, and who may submit their application to Citizenship and Immigration offices in the United States.

Le tableau 8 montre le temps qu'il a fallu au SCRS pour établir les avis d'évaluation qu'il remet à l'égard des demandes du gouvernement et des demandes d'évaluation de sécurité à l'immigration, s'il ne trouve aucun renseignement défavorable au sujet du demandeur.

TABLEAU 8
DÉLAIS (EN JOURS) DU SCRS À FOURNIR DES AVIS D'ÉVALUATION

	2006-2007	2007-2008	2008-2009
Citoyenneté	1	1	1
Immigration (du Canada)*	78	59	95
Immigration (des États-Unis)**	29	45	65
Immigration (de l'étranger)	14	20	26
Détermination du statut de réfugié	98	64	89
Contrôle de sécurité préliminaire	19	28	29

* Comprend certaines catégories de personnes qui demandent, au Canada, le statut de résident permanent.
** Comprend les personnes admises légalement au Canada depuis au moins un an et pouvant présenter des difficultés aux bureaux de Citoyenneté et Immigration aux États-Unis.

Evaluations de sécurité à l'immigration

Ce type d'autorisation aide à veiller à ce que les individus qui posent une menace à la sécurité et/ou qui sont interdits de territoire, selon la *Loi sur l'immigration et la protection des réfugiés*, ne puissent entrer au Canada ni y obtenir un statut. Si un individu répond à l'un ou à plusieurs de ces critères, le SCRS remet une note. Le tableau 7 fait état du nombre de demandes d'évaluation de sécurité à l'immigration, reçues de Citoyenneté et Immigration par le SCRS, et des notes auxquelles ont donné lieu ces demandes.

TABLEAU 7 DEMANDES D'ÉVALUATION DE SÉCURITÉ À LA CITOYENNETÉ ET À L'IMMIGRATION PAR LE SCRS ET NOTES REMISES						
Demandes*		Notes				
2006- 2007	2007- 2008	2008- 2009	2006- 2007	2007- 2008	2008- 2009	

Résident permanent†	62 800	66 000	67 300	201	195	213
Contrôle de sécurité préliminaire††	17 900	21 800	26 800	143	117	108
Détermination du statut de réfugié†††	11 600	6 600	6 600	153	142	102
Total partiel	92 300	94 400	100 700	497	454	423
Demandes de citoyenneté	227 300	190 000	169 500	155	109	169
Total	319 600	284 400	270 200	652	563	592

* Chiffres arrondis à la centaine la plus proche.
† Comprend les demandes de résidents permanents au Canada et à l'étranger (à l'exclusion du Programme de détermination du statut de réfugié), de résidents permanents aux États-Unis et de demandeurs à l'étranger.
†† Demandeurs du statut de réfugié au Canada ou aux points d'entrée.
††† Réfugiés, selon la définition de la LIPR, qui demandent au Canada le statut de résident permanent.

Évaluations de sécurité en vue de l'accès à des sites

Ce type d'autorisation permet à son détenteur d'accéder à certaines zones sécurisées — tels les aéroports, les ports et installations maritimes, la Cité parlementaire et les centrales nucléaires — ou l'accrédite en vue d'un événement spécial. Il permet en outre de fournir des évaluations aux ministères provinciaux. Ces programmes visent à renforcer la sécurité et à réduire la menace possible des groupes terroristes et des gouvernements étrangers qui, sans autorisation, peuvent chercher à se procurer des renseignements classifiés ou d'autres biens, ou à avoir accès à des documents ou à des sites délicats. Le tableau 6 fait état du nombre de demandes d'autorisation d'accès à des sites que le SCRS a reçues au cours du dernier exercice par rapport aux deux précédents.

TABLEAU 6 DEMANDES D'AUTORISATION D'ACCÈS À DES SITES AU SCRS*			
	2006-2007	2007-2008	2008-2009

Cité parlementaire	1 100	1 100	1 000
Zones réglementées d'aéroports (Transports Canada)	39 300	36 800	31 400
Centrales nucléaires	17 900	9 200	11 100
Expéditions rapides et sécuritaires (EXPRES)	23 100	10 700	6 400
Accréditation en vue d'événements spéciaux	0	1 300	16 300
Programme d'habilitation de sécurité en matière de transport maritime [†]	S.O.	6 300	5 200
Autres ministères fédéraux	2 500	2 100	2 600
Total	83 900	67 500	74 000

* Chiffres arrondis à la centaine la plus proche.

[†] Le Programme d'habilitation de sécurité en matière de transport maritime, entré en vigueur en décembre 2007, vise à fournir des évaluations relatives à la sécurité des ports du Canada.

```

prestation de ces évaluations par le SCRS.

```

2006-2007 2007-2008 2008-2009

Demandes du ministère
de la Défense nationale (MDN)

* Chiffres arrondis à la centaine la plus proche

centrales nucléaires

LES ÉVALUATIONS DE SÉCURITÉ

2006-2007+ 2007-2008 2008-2009

Nouvelles Mises à jour

types d'évaluations

Mandats

Le pouvoir d'autoriser des méthodes d'enquête intrusives appartient exclusivement à la Cour fédérale du Canada. Le tribunal qui décerne un mandat au SCRS l'autorise à recourir à des méthodes d'enquête qui seraient illégales autrement, par exemple l'interception de télécom-muniquions. Le tableau 3 indique le nombre de mandats que la Cour fédérale a octroyés au SCRS pendant la période à l'étude, par rapport aux exercices financiers précédents.

TABLEAU 3 STATISTIQUES SUR LES MANDATS			
	2006-2007	2007-2008	2008-2009

Mandats nouveaux	42	71	26
Mandats remplacés ou renouvelés	134	182	183
Total	176 [†]	253 ^{††}	209 ^{†††}

[†] Comprend 25 mandats urgents.

^{††} Comprend 19 mandats urgents.

^{†††} Comprend 2 mandats urgents.

B. ACTIVITÉS EN MATIÈRE D'ÉVALUATION
DE SÉCURITÉ

Les évaluations de sécurité constituent l'une des fonctions du SCRS les mieux connues du public. Elles peuvent être faites pour le gouvernement (et comprennent alors le contrôle autorisant l'accès à des sites) ou relativement à l'immigration.

Évaluations de sécurité pour le gouvernement

Ce type de contrôle fournit les évaluations de sécurité requises — évaluation de la loyauté d'un individu envers le Canada et (à cet égard) de sa fiabilité — à toutes les institutions et à tous les ministères fédéraux, à l'exception de la Gendarmerie royale du Canada.

Le SCRS ne décide pas qui doit se voir octroyer une habilitation de sécurité. Il informe plutôt le ministre ou organisme demandeur des renseignements qui pourraient infléchir sa décision d'accorder une habilitation. En de rares occasions, le SCRS fait état du fait que les critères de la Politique du gouvernement sur la sécurité sont remplis pour le refus d'une habilitation. Cependant, il incombe au demandeur d'octroyer, de révoquer ou de refuser l'habilitation.

Chaque année, dans le cadre du rapport annuel du CSARS, le Comité fait état d'importants renseignements et statistiques ayant trait aux opérations du SCRS. Ces données, qui lui viennent du Service, donnent au lecteur un éclairage sur certaines fonctions principales de celui-ci et font ressortir les grands changements ou les faits nouveaux survenus au sein du SCRS.

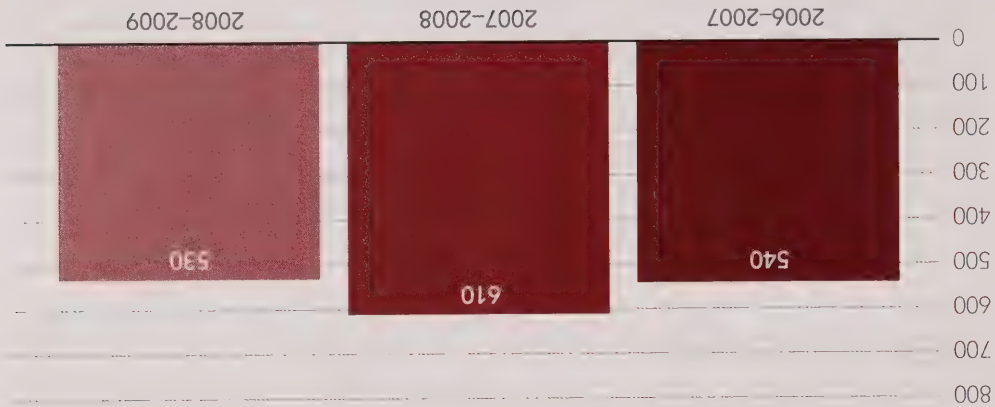
Pour le rapport annuel 2008-2009 du CSARS, ces renseignements sont regroupés en deux catégories : les activités en matière de renseignement de sécurité et celles en matière d'évaluation de sécurité.

A. ACTIVITÉS EN MATIÈRE DE RENSEIGNEMENT DE SÉCURITÉ

Ciblage

Si le Service a des motifs raisonnables de soupçonner qu'un individu ou une organisation peut représenter une menace pour le Canada, il doit d'abord instituer une enquête au cours de laquelle il exerce des pouvoirs proportionnels à cette menace. La figure 1 indique le nombre de cibles qui ont fait l'objet d'enquêtes du SCRS pendant la période à l'étude, par rapport aux exercices financiers précédents.

FIGURE 1
STATISTIQUES SUR LES ENQUÊTES*



Note : * Chiffres arrondis à la dizaine la plus proche.

ANNEXE A : LISTE DES RECOMMANDATIONS

Pendant l'exercice 2008-2009 qui est observé, le CSARS a formulé les recommandations suivantes qui découlent des diverses études qu'il a effectuées et de la plainte sur laquelle il a enquêté.

AFFAIRE : LE CSARS A RECOMMANDÉ QUE...

ROLE JOUÉ PAR LE SCRS DANS L'AFFAIRE OMAR KHADR

Le Service devrait songer à élaborer un cadre stratégique destiné à guider ses interactions auprès des jeunes. Dans ce cadre-là, il devrait veiller à ce que ces interactions se fonde sur le même type de principes que ceux consacrés en droit canadien et international.

Le SCRS devrait instaurer des mesures pour intégrer dans son travail courant les valeurs découlant des faits récents sur la scène politique, judiciaire et juridique, afin de maintenir sa propre crédibilité et de combler les attentes croissantes et changeantes quant aux modalités d'opération et de rendement d'un service de renseignement dans une société démocratique contemporaine. Les conseils et l'assistance du ministre de la Sécurité publique seraient utiles quant à la manière de s'acquitter de cette tâche.

ACTIVITÉS DU SCRS AUX AÉROPORTS INTERNATIONAUX DU CANADA

Le SCRS devrait soutenir les efforts visant à favoriser une collaboration plus grande entre les membres de son personnel afin d'améliorer leurs activités opérationnelles dans les aéroports canadiens.

Le Service devrait veiller à ce que ses plans de gestion des catastrophes englobent les activités aéroportuaires de façon à disposer de procédures visant à mieux assurer que les services essentiels offerts ne soient pas interrompus dans le cas où ses bureaux deviendraient inutilisables.

OPÉRATION DU SCRS FAISANT APPEL À DES SOURCES HUMAINES

Le SCRS devrait informer le ministre de la Sécurité publique des implications de la *Loi antiterroriste* en ce qui a trait à son programme des sources humaines et à tout futur fait nouveau connexe.

ACTIVITÉS DU SCRS DANS UN POSTE À L'ÉTRANGER

Le SCRS devrait prendre des mesures afin de définir de façon plus solide et de mieux comprendre le contexte de l'extrémisme lié à la défense de causes multiples. L'objectif devrait être de concevoir un modèle plus efficace afin d'isoler et d'identifier les indicateurs de l'extrémisme activiste et de sa propension à la violence.

Pour la liste de toutes les études menées par le CSARS depuis 1984, veuillez consulter son site Web, à l'adresse suivante : www.sifc-csars.gc.ca

l'année. La marche des affaires courantes est confiée au directeur exécutif qui s'enquiert au besoin de la ligne de conduite à tenir auprès du président, premier dirigeant du CSARS. Dans le cadre de leurs travaux suivis, le président et les membres du Comité ainsi que les cadres supérieurs prennent part à des discussions régulières avec la direction et le personnel du SCRS et avec d'autres membres de haut rang de la collectivité du renseignement de sécurité.

À ces échanges se greffent des discussions avec des universitaires et des experts du renseignement et de la sécurité et avec d'autres organismes compétents. Ces activités visent à enrichir les connaissances du CSARS au sujet des dossiers et opinions qui intéressent le renseignement concernant la sécurité nationale.

Les membres du Comité visitent aussi les bureaux régionaux du Service à tour de rôle pour mieux comprendre et examiner le travail courant des enquêteurs locaux. Ces visites leur fournissent l'occasion de se faire exposer les problèmes, difficultés et priorités propres à ces bureaux par les cadres régionaux du Service. Elles leur permettent aussi de faire valoir ce qui polarise les efforts et les préoccupations du CSARS.

Au cours de l'exercice 2008-2009, les membres du CSARS se sont rendus dans trois bureaux régionaux.

BUDGET ET DÉPENSES

Le CSARS continue de gérer ses activités dans les limites des ressources qui lui sont octroyées. Ses principales dépenses ont trait au traitement et aux déplacements de ses membres et de son personnel au Canada pour prendre part aux audiences, exposés et activités de surveillance du Comité. Le tableau 2 présente une ventilation des prévisions de dépenses et des dépenses réelles.

TABLEAU 2 DÉPENSES DU CSARS 2008-2009		
	2008-2009 (prévisions)	2008-2009 (réelles)
Personnel	1 900 000 \$	1 700 000 \$
Biens et services	1 000 000 \$	700 000 \$
Total	2 900 000 \$	2 400 000 \$

COMPOSITION DU COMITÉ

La présidence du CSARS est occupée par l'honorable Gary Filmon, C.P., O.M., nommé à cette charge le 24 juin 2005. Les autres membres du Comité sont l'honorable Frances Lankin, C.P., l'honorable Denis Losier, C.P., l'honorable Arthur T. Porter, C.P., M.D., et l'honorable Raymond Speaker, C.P., O.C.

Tous les membres du CSARS font partie du Conseil privé et sont nommés par le gouverneur en conseil après consultation entre le premier ministre et les chefs des partis de l'opposition.

En plus d'assister aux réunions mensuelles du Comité, les membres président les audiences de plaintes, préparent des études et des rapports de plaintes en consultation avec le personnel du CSARS, visitent les bureaux régionaux du SCRS, comparatissent devant des comités parlementaires et exercent d'autres fonctions liées à leurs responsabilités.

PERSONNEL ET ORGANISATION

Le CSARS jouit du soutien de son directeur exécutif, Susan Pollak, et d'un effectif autorisé de 20 employés, en poste à Ottawa. Son personnel est ainsi composé : un conseiller principal, un avocat principal, un directeur des services généraux, un avocat, un parajuriste principal ainsi que des chercheurs et des employés de soutien administratif.

Les membres du Comité dicent au personnel l'orientation à donner aux travaux de recherche et autres activités, désignées prioritaires pour

ACTIVITÉS DU COMITÉ

5-8 octobre 2008 : Le président, le directeur exécutif et un membre du CSARS ont assisté à la conférence internationale des organismes de surveillance tenue à Auckland, en Nouvelle-Zélande, par l'inspecteur général, Intelligence and Security.

30 octobre-1^{er} novembre 2008 : Le directeur exécutif et plusieurs membres du personnel ont assisté à une conférence tenue à Ottawa par l'Association canadienne pour l'étude de la sécurité et du renseignement.

4 novembre 2008 : Le directeur exécutif a prononcé une conférence devant des étudiants de l'Université Carleton, inscrits à un cours sur la sécurité nationale, leur donnant un aperçu du rôle et du mandat du CSARS.

5 mars 2009 : Le directeur exécutif a comparu devant le Comité permanent de la Chambre des communes sur la sécurité publique et nationale.

24 mars 2009 : L'avocat principal par intérim et le conseiller principal ont rencontré des représentants du Service néo-zélandais du renseignement de sécurité.

26 mars 2009 : L'avocat principal par intérim et le conseiller principal ont rencontré des représentants du Intelligence Security Committee (Royaume-Uni).

LE POUVOIR LÉGAL DU CSARS
D'ENQUÊTER SUR LES PLAINTES

En vertu de l'article 41 de la Loi sur le SCRS, le CSARS est autorisé à enquêter sur les plaintes que « toute personne » peut porter contre « des activités du Service ». Il doit aussi être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet ni entachée de mauvaise foi.

À PROPOS DE LA POLITIQUE DU
GOUVERNEMENT SUR LA SÉCURITÉ

Le gouvernement du Canada doit veiller à ce que les personnes qui ont accès aux renseignements et aux biens du gouvernement soient fiables et loyales. Il est essentiel d'assurer la loyauté envers le Canada pour protéger la population canadienne et ses biens contre les menaces que représentent le terrorisme et l'espionnage, ou contre les activités malveillantes ou malhonnêtes, telle la communication non autorisée de renseignements classifiés et protégés, qui peuvent avoir de sérieuses répercussions sur la sécurité des Canadiens et sur le bon fonctionnement de la société. Les ministères fédéraux doivent donc veiller à ce que les candidats soient soumis à une évaluation de sécurité appropriée avant d'entrer en fonction. Le SCRS joue un rôle vital dans ce processus par les évaluations de sécurité qu'il effectue pour les institutions et ministères fédéraux (pour de plus amples renseignements sur les activités du SCRS en matière d'évaluation de sécurité, voir l'annexe B du rapport). Vous trouverez d'autres détails concernant la Politique du gouvernement sur la sécurité sur le site Web du Secrétariat du Conseil du Trésor du Canada (www.tbs-sct.gc.ca).

et qui auraient été interdites en vertu de la *Charte canadienne des droits et libertés*. Le plaignant a demandé des excuses et l'assurance écrite que le SCRS cesserait de poser de telles questions lors des futures entrevues d'évaluation de sécurité.

Pour sa part, le SCRS a affirmé qu'il ne lui était pas inhabituel de tenir des entrevues dans le cadre du processus d'évaluation de sécurité. On peut mener des entrevues pour un motif valable si l'on estime ne pas avoir suffisamment de renseignements au sujet d'une personne pour effectuer une évaluation de sécurité. Lors de l'évaluation même, le SCRS est tenu, de par la *Loi sur le SCRS*, d'évaluer « la loyauté d'un individu envers le Canada et, à cet égard, [...] sa fiabilité ». Ce faisant, au moment d'effectuer ces évaluations, il prend en considération une foule de facteurs dont les croyances et les relations de l'intéressé — questions qu'il estime être dans la foulée de la Politique du gouvernement sur la sécurité, du Secrétariat du Conseil du Trésor.

L'enquête du CSARS comprenait un examen détaillé des documents du SCRS et des témoignages du plaignant, des représentants du SCRS et d'un représentant du Secrétariat du Conseil du Trésor, qui a parlé de l'objectif de la Politique du gouvernement sur la sécurité. Ces renseignements ont convaincu le CSARS qu'en demandant que le plaignant subisse une entrevue d'évaluation de sécurité, le SCRS s'était conformé à la Politique du gouvernement sur la sécurité, à la norme de cette politique et à sa propre politique opérationnelle applicable. De plus, le CSARS a constaté que le plaignant n'avait pas fait l'objet d'un profilage pour des motifs interdits par la *Charte canadienne des droits et libertés* et que les questions qu'il s'était vu poser à l'entrevue d'évaluation de sécurité au sujet de ses opinions et croyances ne lésaient pas ses droits protégés par la *Charte*.

DÉTERMINATION DE LA COMPÉTENCE DU CSARS À EXAMINER UNE PLAINTÉ...

...EN VERTU DE L'ARTICLE 41

...EN VERTU DE L'ARTICLE 42

Quant aux habilitations de sécurité, le CSARS est tenu, selon l'article 42 de la *Loi sur le SCRS*, d'enquêter sur les plaintes présentées par :

1. les personnes qui ne sont pas embauchées par le gouvernement fédéral à cause du refus d'une habilitation de sécurité;

2. les fonctionnaires fédéraux qui sont renvoyés, rétrogradés ou mutés ou qui se voient refuser une promotion ou une mutation pour la même raison;

3. les personnes qui se voient refuser un contrat pour la fourniture de biens ou de services au gouvernement, toujours pour le même motif.

Les plaintes de ces types doivent être présentées dans les 30 jours du refus de l'habilitation de sécurité. Le CSARS peut prolonger cette période si des raisons valables lui sont fournies.

Selon l'article 41 de la *Loi sur le SCRS*, le CSARS est tenu de faire enquête sur les plaintes que « toute personne » peut porter contre « des activités du Service ». Pour que le CSARS fasse enquête, deux conditions doivent être remplies :

1. le plaignant doit d'abord avoir présenté sa plainte par écrit au directeur du SCRS sans recevoir de réponse dans un délai raisonnable (environ 30 jours) ou, s'il en a reçu une, sans que cette réponse le satisfasse;
2. le CSARS doit être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet ni entachée de mauvaise foi.

Le CSARS ne peut enquêter sur une plainte qui peut être réglée autrement, par une procédure de griefs en vertu de la *Loi sur le SCRS* ou de la *Loi sur les relations de travail dans la fonction publique*.

Plainte présentée au CSARS : Enquête sur une affaire de profilage présumé

Le CSARS a enquêté sur une plainte dont l'auteur devait obtenir une autorisation d'accès aux zones réglementées d'aéroports pour obtenir un emploi. Dans cette affaire, Transports Canada a demandé au SCRS d'effectuer une évaluation de sécurité en vue d'établir la loyauté de cet individu envers le Canada et, à cet égard, sa fiabilité. Le SCRS s'est ensuite mis en rapport avec le plaignant et lui a fait subir une entrevue d'évaluation de sécurité. Dans la plainte présentée au CSARS en vertu de l'article 41 de la *Loi sur le SCRS*, l'auteur a prétendu que le SCRS avait fait du profilage. De plus, il s'est opposé à l'utilisation, pendant l'entrevue, de questions qui visaient à son avis à connaître ses opinions politiques

Lorsque le CSARS termine son enquête sur une plainte relevant de l'article 41, il présente un rapport au directeur du SCRS, au ministre de la Sécurité publique et au plaignant¹. Les résumés des rapports de plaintes, expurgés de manière à protéger la sécurité nationale et la vie privée des intéressés, figurent également dans le rapport annuel du CSARS au Parlement.

Selon l'article 42 de la *Loi sur le SCRS*, les personnes à qui une habilitation de sécurité est refusée doivent être informées de cette décision par l'administrateur général de leur organisme. Elles ont le droit de porter plainte auprès du CSARS et, s'il y a lieu, celui-ci fait enquête et présente ses constatations et recommandations au Ministre, au directeur du SCRS, à l'administrateur général compétent et au plaignant.

Si un ministre avise par écrit la Commission canadienne des droits de la personne d'une plainte qui a trait à la sécurité du Canada, elle peut en saisir le CSARS. Le cas échéant, ce dernier effectue une enquête et fait rapport de ses constatations à la Commission, au directeur du SCRS, au ministre de la Sécurité publique, au ministre compétent et au plaignant. Le CSARS a aussi le pouvoir d'enquêter sur les affaires dont il est saisi en vertu de la *Loi sur la citoyenneté*.

Le tableau 1 fait état de toutes les plaintes qui ont été présentées au CSARS au cours des trois derniers exercices financiers, y compris celles qui lui avaient été adressées à tort, qui ont été déclarées hors de sa compétence ou qui ont fait l'objet d'une enquête ou d'un règlement sans audience (p. ex., par un examen administratif).

TABLEAU 1
RÈGLEMENT DES PLAINTES

	2006-2007	2007-2008	2008-2009
Reportées de l'exercice précédent	24	20	15
Nouvelles	37	32	30
Total	61	52	45
Dossiers réglés†	41	37	23
Reportées à l'exercice suivant	20	15	22
Rapports	5	6	1

† L'égard desquels des rapports ont été présentés au CSARS. Les dossiers réglés comprennent les dossiers traités par le CSARS, les dossiers traités par le SCRS, les dossiers traités par le ministre de la Sécurité publique et les dossiers traités par le ministre de la Justice. Les dossiers traités par le CSARS sont ceux dont les plaintes ont été déclarées hors de sa compétence ou qui ont fait l'objet d'une enquête ou d'un règlement sans audience (p. ex., par un examen administratif).

SECTION 2 : RÉSUMÉS DES ÉTUDES DU CSARS ET DES PLAINTES

B. PLAINTES

Outre sa fonction de surveillance, le CSARS a charge d'enquêter sur les plaintes contre le SCRS. La première étape de presque tout dossier de plainte est une demande de renseignements présentée au CSARS — soit par écrit, en personne ou au téléphone. À ces demandes, le personnel du CSARS répond sur-le-champ en indiquant généralement au plaignant éventuel ce que la *Loi sur le SCRS* exige pour que son affaire soit considérée à titre de plainte officielle.

QUELLE EST LA DIFFÉRENCE ENTRE UNE ÉTUDE ET UNE ENQUÊTE SUR UNE PLAINTÉ?

Une **étude** est amorcée par le CSARS et entraîne des recherches approfondies sur la manière dont le Service s'acquitte de ses fonctions, décrites dans la *Loi sur le SCRS*. Une enquête sur une plainte est mise en branle par : une **plainte** qu'une personne ou un groupe porte auprès du CSARS contre « des activités » du Service (article 41); le refus ou le retrait d'une habilitation de sécurité à un fonctionnaire ou à un fournisseur de l'État (article 42); un renvoi de la Commission canadienne des droits de la personne; et un rapport du Ministère en ce qui concerne la *Loi sur la citoyenneté*. Les études entrent dans la fonction de recherche du CSARS, alors que les enquêtes sur les plaintes sont menées dans le cadre d'un processus quasi judiciaire.

TYPES DE PLAINTES

L'équipe de juristes du CSARS fournit des avis concernant la procédure et les questions de fond et il contre-interroge aussi les témoins du SCRS si, pour des raisons de sécurité nationale, les témoignages doivent être entendus en l'absence du plaignant. Les types de plaintes sur lesquelles le CSARS fait enquête sont décrits dans la *Loi sur le SCRS* et peuvent prendre diverses formes. En vertu de l'article 41 de cette loi, le CSARS peut instruire les plaintes sur n'importe quelles « activités du Service ». Selon l'article 42, il peut entendre celles qui ont trait au refus d'habilitations de sécurité à des employés ou à des fournisseurs du gouvernement fédéral. Ce dernier article n'autorise pas le CSARS à se déclarer compétent pour instruire les plaintes concernant les contrôles d'antécédents ou vérifications de fiabilité moins intrusifs qui visent simplement à déterminer la fiabilité et les qualifications d'un candidat à un poste dans la fonction publique fédérale. Ces plaintes sont régies au moyen de la procédure de griefs établie pour un organisme ou, peut-être, en vertu de l'article 41 de la *Loi sur le SCRS*.

qui ont présenté Hampel comme un agent du renseignement russe vivant au Canada sous une fausse identité depuis 1995. Cependant, il n'y a eu aucun reportage sur la nature et la portée de la participation du SCRS à cette affaire très médiatisée et délicate.

L'ÉTUDE DU CSARS

Dans son étude, le CSARS a cherché à comprendre le rôle joué par le SCRS dans l'affaire Hampel. Il a constaté qu'une fois au fait de l'existence de Hampel, le SCRS avait mené une enquête pour déterminer la nature et la portée des activités d'espionnage de l'intéressé.

Au cours de son enquête, le Service a reçuilli d'importants renseignements qui lui ont permis d'informer les ministres de la Sécurité publique et de la Citoyenneté et de l'Immigration du fait que Hampel était un membre connu du Service du renseignement extérieur russe et qu'il utilisait une fausse identité canadienne pour contribuer aux activités d'espionnage de la Russie. Conformément à la *Loi sur l'immigration et la protection des réfugiés*, les ministres ont signé une attestation de sécurité qui a mis en branle le processus de l'expulsion éventuelle de Hampel vers la Russie.

Grâce à son enquête sur Hampel, le SCRS a acquis un nouvel éclairage sur les menaces d'espionnage que les activités des services de renseignement russes représentaient pour le Canada. Cela l'aidera à enquêter sur les menaces semblables qui pourraient survenir.

Aucune recommandation ne découle de cette étude.

Le deuxième objectif était d'examiner les enquêtes du SCRS sur des événements spéciaux (ceux suscitant davantage d'occasions propices à des activités liées à la menace). À cet égard, le Comité a examiné les plans et priorités arrêtés par le Service en vue des Jeux olympiques et paralympiques d'hiver de 2010, à Vancouver, et il a constaté qu'ils arrivaient à point nommé et étaient bien conçus. Cependant, plusieurs préoccupations soulevées dans le contexte de l'enquête sur l'extrémisme intérieur — concepts clés qui ne jouissent pas d'une définition commune ou ne sont pas utilisés de façon uniforme — valaient aussi pour l'évaluation, par le Service, du contexte de la menace entourant les Jeux olympiques et paralympiques.

Il est important de noter que la compréhension du contexte de la menace relative aux Jeux olympiques, par le SCRS, continue d'évoluer et que l'efficacité du Service pendant les Jeux de 2010 dépendra de sa capacité d'évaluer avec exactitude les mouvements associés à l'extrémisme intérieur. Le CSARS croit que les stratégies recommandées pour faire face aux préoccupations révélées par l'enquête sur l'extrémisme intérieur éclaireront aussi les préparatifs du SCRS en vue des Jeux olympiques.

SOMMAIRE DES RECOMMANDATIONS

- Une recommandation découle de cette étude.
- Le SCRS devrait prendre des mesures afin de définir de façon plus solide et de mieux comprendre le contexte de l'extrémisme lié à la défense de causes multiples. L'objectif devrait être de concevoir un modèle plus efficace afin d'isoler et d'identifier les indicateurs de l'extrémisme activiste et de sa propension à la violence.

Étude du CSARS : L'affaire Paul William Hampel

CONTEXTE

L'ancien directeur du SCRS, Jim Judd, a reconnu publiquement que l'espionnage étranger prend une forme de plus en plus sophistiquée en sol canadien. Une affaire récente d'espionnage russe au Canada souligne cette préoccupation. En novembre 2006, des responsables canadiens ont placé en détention à Montréal un espion russe qui se faisait appeler Paul William Hampel, au moment où il s'apprêtait à s'envoler pour l'étranger. Les circonstances de sa détention ont suscité une vive attention des médias

Étude du CSARS : Enquête du SCRS sur l'extrémisme intérieur

CONTEXTE

Le gouvernement du Canada considère l'extrémisme intérieur comme une priorité du renseignement national. Voilà pourquoi le SCRS fait de la violence intérieure à caractère politique l'une de ses toutes premières priorités. L'enquête sur l'extrémisme intérieur présente cependant pour lui un défi unique. Le Service doit recueillir les renseignements dont il a besoin pour remplir son mandat, mais il doit aussi se garder de léser le droit protégé des Canadiens aux activités de défense d'une cause, de protestation ou de manifestation d'un désaccord. Pour bien tracer la ligne de démarcation entre les activités licites de protestation et l'extrémisme activiste, il faut une compréhension spécialisée et approfondie des mouvements de défense de causes, des tactiques de protestation et des manières dont des protestataires autrement bien intentionnés peuvent se radicaliser.

L'ÉTUDE DU CSARS

Cette étude comportait deux objectifs. Tout d'abord, le CSARS a examiné les activités du SCRS relativement à l'extrémisme intérieur, compte tenu de l'empêchement sur les enquêtes criminelles et les activités de défense d'une cause, de protestation et de manifestations d'un désaccord. Le CSARS a constaté que le SCRS avait déployé des ressources appropriées face à la menace possible de l'extrémisme intérieur. De plus, celui-ci avait acquis une expertise poussée quant aux menaces éventuelles de l'extrémisme intérieur et il avait pris une série de mesures équilibrées pour assurer aux Canadiens le droit de manifester leur dissidence de façon licite.

Cependant, le CSARS a constaté que certaines stratégies employées par le Service pour analyser le contexte de la menace gagneraient à être redéfinies. Plusieurs concepts clés servant à évaluer la menace possible ne sont pas compris par tous ou utilisés de façon uniforme, ou ne jouissent pas d'une définition commune. Le CSARS a recommandé que le Service arrête une terminologie acceptée et acquière une compréhension plus approfondie des paramètres du contexte de la menace afin d'isoler et d'identifier les indicateurs de la radicalisation.

en dépit des contraintes budgétaires. La Direction des STS relève ces défis en collaborant avec les partenaires du gouvernement du Canada et en sous-traitant auprès de l'industrie. Au cours de l'étude du CSARS, il est devenu manifeste que les STS n'ont pas en main tout ce qu'il faut pour relever les défis auxquels ils font face. Le principal de ces défis est la nécessité de suivre l'évolution rapide des technologies dans diverses disciplines. Un défi connexe est l'absence de législation sur l'accès légal, ce qui oblige les fournisseurs de services de télécommunications à doter leurs produits d'une capacité d'interception. Ceci diffère radicalement de l'expérience des homologues du SCRS aux États-Unis et en Europe où les gouvernements ont adopté des mesures législatives sur la coopération entre les prestataires de services et les organes de renseignement de sécurité.

Au Canada, les opposants à la loi sur l'accès légal expriment diverses préoccupations dont :

- la pertinence d'obliger les fournisseurs de services à créer des solutions d'interception;
- la portée des renseignements qui seraient obtenus et l'usage qu'on en ferait;
- l'existence possible de restrictions ou d'un contrôle pour prévenir les abus.

La commissaire à la protection de la vie privée du Canada s'est prononcée contre diverses

itérations de la loi proposée, affirmant tout récemment : « L'accès légal soulève des questions fondamentales concernant les droits, comme le droit à la vie privée et le droit de communiquer librement ». Le Comité reconnaît l'importance de l'engagement des Canadiens dans un débat sain sur cette question. Cependant, il craint que la capacité des STS d'exécuter certaines procédures d'enquête ne demeure limitée tant que le gouvernement n'aura pas réussi à adopter une loi appropriée.

Aucune recommandation ne découle de cette étude.

Le 18 juin 2009, pendant la préparation du rapport annuel 2008-2009 du CSARS, le gouvernement fédéral a déposé la Loi sur l'assistance au contrôle d'application des lois au 21^e siècle. Si cette mesure est adoptée, elle obligera les fournisseurs de services Internet à doter leurs réseaux d'une capacité d'interception. Le CSARS suivra l'élaboration de cette loi afin d'en déterminer les effets possibles sur le mandat et les priorités du Service en matière de collecte de renseignements.

Comme l'activité des postes du SCRS s'intensifie sur le plan opérationnel, ils répondent à certains besoins que comblerait autrement un service de renseignement étranger distinct. Le CSARS continuera de surveiller à la fois les activités du Service et celles de ces postes à mesure qu'ils assument des rôles opérationnels élargis.

SOMMAIRE DES RECOMMANDATIONS

Une recommandation découle de cette étude.

- Pour le partage d'informations avec les partenaires étrangers, le SCRS devrait veiller à l'application plus générale de la pratique acceptée, qui consiste à acheminer tous les messages par l'entremise des postes compétents du SCRS à l'étranger.

Étude du CSARS : Services techniques et scientifiques du SCRS

CONTEXTE

De toutes les stratégies employées par le SCRS pour recueillir des renseignements et y avoir accès, celles qui reposent sur la technologie sont considérées comme exigeant le plus de ressources. La conception et le déploiement de ces technologies requièrent un vaste éventail de spécialités, dont la médecine légale, le génie mécanique, la programmation et l'analyse en laboratoire. Ces spécialités entrent toutes dans le cadre des responsabilités de la Direction des services techniques et scientifiques (STS) du SCRS.

Le CSARS avait déjà examiné certains aspects des opérations techniques du Service dans de précédentes études, mais il estimait judicieux d'effectuer une analyse plus approfondie de ce qui se fait dans l'ombre au SCRS avant l'exécution d'une opération.

L'ÉTUDE DU CSARS

L'objectif de cette étude était de mieux comprendre la nature et la portée des travaux de la Direction des STS, y compris les défis qu'il lui faut relever pour exécuter son travail et sa façon de coopérer avec divers partenaires. La technologie du renseignement est une affaire complexe qui exige un accès continu à de nouveaux talents et à une recherche-développement novatrice, de même que la capacité d'élaborer des produits rapidement

étrangers du SCRS et le filtrage des demandes d'immigration. De plus, les représentants du SCRS à l'Administration centrale avaient l'habitude de gérer les opérations hors du pays. Aujourd'hui, cependant, les postes du SCRS jouent à cet égard un rôle élargi qui coïncide avec un accroissement du nombre d'opérations du SCRS à l'étranger, comme le soulignait l'ancien directeur du SCRS, Jim Judd, qui a reconnu publiquement la participation du SCRS à des opérations en Afghanistan, en Irak et au Liban.

L'ÉTUDE DU CSARS

Cette année, le Comité a examiné les activités d'un poste du SCRS à l'étranger, chargé des relations du Service avec des organismes de divers pays. Même s'il ne s'agit pas de l'un des postes les plus occupés, le travail qui s'y faisait laissait entrevoir un degré élevé de coopération et d'échange de renseignements. Le poste examiné prenait part activement à diverses opérations qui, pour la plupart, étaient toujours gérées par des représentants au Canada. Par conséquent, le travail de liaison demeurait sa tâche principale. Néanmoins, le CSARS a noté que le poste jouit d'une position enviable quant à l'exercice de son mandat en matière de liaison et d'opérations.

Pour gérer efficacement les relations avec l'étranger, tous les postes du SCRS doivent avoir des méthodes efficaces de partage d'informations, à la fois avec le SCRS et avec ses organismes partenaires. Le CSARS a relevé trois défis ayant trait aux communications, au poste à l'étude. Dans deux cas, ces défis ont causé des inconvénients sans toutefois empêcher le personnel sur place de faire son travail. Le CSARS a aussi noté que le SCRS avait déjà indiqué qu'il avait entrepris de trouver des solutions à ces questions.

Le troisième défi avait trait au transfert direct d'informations de l'Administration centrale du SCRS aux représentants d'organismes étrangers, au lieu de la pratique acceptée consistant à acheminer les informations par l'entremise des postes compétents du SCRS. Le CSARS a indiqué qu'il aimerait que l'on recoure de façon plus générale à la pratique acceptée pour le transfert d'informations (c.-à-d. la transmission de tous les messages par les postes compétents du SCRS).

Lorsque le Service entreprend des opérations à l'étranger, l'approbation d'un niveau supérieur est requise au SCRS. Au cours des dernières années, ce processus d'approbation a été délégué vers le bas. Le nouveau processus, cependant, est ambigu et rend incohérente la démarche des demandes d'approbation, dans certains cas. Le SCRS a instauré récemment de nouveaux processus qui débordent toutefois la portée des travaux du CSARS pour la période à l'étude. Néanmoins, il vaut la peine de noter que, selon l'estimation du CSARS, la délégation de pouvoirs est un important fait nouveau qui mérite d'être examiné plus avant.

Sur le plan de la responsabilité au sein du SCRS, la politique opérationnelle n'a pas été mise à jour afin d'englober les nouveaux facteurs qu'il faut examiner pour déterminer si des activités menées dans le cadre du programme des sources humaines sont licites. Néanmoins, le CSARS a constaté que le Service s'était doté d'une structure redditionnelle propre à assurer des discussions utiles sur les questions importantes qui touchent la gestion de ce programme.

Quant à la reddition de comptes au ministre de la Sécurité publique, le CSARS a constaté qu'en raison de l'interprétation de la politique opérationnelle par le SCRS et, par extension, de la mise en œuvre qu'il en fait, il ne disposait d'aucun moyen d'informer le Ministre des implications de la *Loi antiterroriste* pour les opérations faisant appel à des sources humaines. Le CSARS a proposé un processus visant à faire le point régulièrement sur cette question avec le Ministre.

Depuis l'adoption de la *Loi antiterroriste*, le gouvernement du Canada a relevé plus de quarante entités terroristes. À mesure que s'allonge la liste de ces entités, on s'attend à une augmentation proportionnelle du nombre des opérations, faisant appel à des sources humaines, qui sont susceptibles de bénéficier à des organisations inscrites. Il est important que le SCRS soit tenu de rendre compte de ces activités.

SOMMAIRE DES RECOMMANDATIONS

Une recommandation découle de cette étude.

- Le SCRS devrait informer le ministre de la Sécurité publique des implications de la *Loi antiterroriste* en ce qui a trait à son programme des sources humaines et à tout futur fait nouveau connexe.

Étude du CSARS : Activités du SCRS dans un poste à l'étranger

CONTEXTE

Dans l'exercice de ses responsabilités légales et opérationnelles, le SCRS maintient une présence à l'extérieur du Canada. L'emplacement des postes du SCRS à l'étranger est classifié, à l'exception de trois d'entre eux, situés à Londres, Paris et Washington. Depuis toujours, la fonction première de ces postes était d'assurer la liaison avec les partenaires

Étude du CSARS : Opération du SCRS faisant appel à des sources humaines

CONTEXTE

Le programme des sources humaines du SCRS est considéré comme un outil de renseignement de sécurité efficace et rentable. Les sources auxquelles il fait appel peuvent souvent éclairer sur les intentions d'une cible — ce que ne font pas les autres méthodes de collecte de renseignements du Service.

LOI ANTITERRORISTE AU SUJET DE LA

La Loi antiterroriste confère au gouvernement du Canada le pouvoir de dresser la liste des entités que l'on croit mêlées à des activités terroristes. Elle a en outre criminalisé le fait de réunir ou de rendre disponibles, directement ou indirectement, des biens ou des services financiers, ou d'autres services connexes, sachant qu'un groupe terroriste les utilisera ou en bénéficiera.

L'ÉTUDE DU CSARS

Les mesures législatives prises à ce jour pour faire échec au terrorisme ont suscité des défis uniques au Service quant à la gestion de son programme des sources humaines. L'un de ces défis découle des dispositions de la *Loi antiterroriste* (2001). En effet, les activités liées à ce programme et susceptibles de bénéficier à des organisations inscrites à titre d'entités terroristes pouvaient, par définition, être des actes criminels. Conscient de la complexité juridique de cette situation, le SCRS a déterminé que l'exécution de son programme des sources humaines respecterait les limites prévues par la loi.

Le Comité avait examiné brièvement cette question dans de précédentes études. À l'époque, il avait accepté la position du Service, à savoir que sa politique opérationnelle englobait bel et bien les divers aspects de la gestion des sources humaines. Néanmoins, le CSARS avait soutenu qu'il continuerait de surveiller ce dossier afin de déceler les problèmes, le cas échéant.

Dans la foulée de cet engagement, le CSARS a jugé important de réexaminer ce dossier à ce moment-ci. Pour cette étude, il a mis un accent particulier sur la pertinence et l'adéquation du niveau de responsabilité au sein du SCRS, à l'égard du programme des sources humaines, et de la reddition de comptes au ministre de la Sécurité publique.

déroulent. Les intervenants des aéroports lui demandent aussi des séances d'information sur les questions liées à la menace et, entre autres, sur le mandat du SCRS à l'égard de la sécurité nationale. Ce personnel prodigue aussi des conseils aux autorités de police en réponse à toute infraction à la sécurité ou à tout incident criminel qui survient dans un aéroport et que l'on soupçonne de présenter un risque pour la sécurité nationale. Dans le cadre du rôle joué par le SCRS à l'égard du Programme d'interception aux points d'entrée, les agents d'immigration des aéroports demandent aussi qu'un employé du SCRS soit présent lorsqu'ils voient en entrevue des passagers soupçonnés de représenter une menace pour la sécurité nationale. Lors de ces entrevues, le personnel du SCRS contrôle les antécédents des intéressés afin de déterminer s'ils ont déjà pris part à des activités liées à la menace. Ces conseils experts sont vitaux pour protéger les aéroports d'entrée.

Le personnel du SCRS a aussi consacré pas mal de temps et d'efforts à tisser et à cultiver les relations avec le milieu des aéroports. En intensifiant ainsi ses relations, il peut appuyer les modules opérationnels des régions et de l'Administration centrale qui doivent avoir accès à l'infrastructure aéroportuaire pour exécuter des opérations.

Le CSARS a noté que les employés affectés par le SCRS aux activités aéroportuaires profiteraient d'échanges accrus avec leurs homologues des aéroports d'autres régions du Canada, qui exercent des fonctions courantes semblables aux leurs. Le CSARS croit qu'il faudrait donner à ces employés, dont les fonctions principales sont d'appuyer la sûreté des aéroports, l'occasion de collaborer et de partager des pratiques exemplaires avec leurs pendantes d'autres aéroports.

En général, le CSARS a constaté que les activités du SCRS dans les aéroports appuient le mandat de celui-ci à l'égard de la sécurité nationale. De plus, elles permettent aux intervenants des aéroports d'avoir facilement accès à l'expertise du SCRS.

SOMMAIRE DES RECOMMANDATIONS

Deux recommandations découlent de cette étude :

- Le SCRS devrait soutenir les efforts visant à favoriser une collaboration plus grande entre les membres de son personnel afin d'améliorer leurs activités opérationnelles dans les aéroports canadiens.
- Le Service devrait veiller à ce que ses plans de gestion des catastrophes englobent les activités aéroportuaires de façon à disposer de procédures visant à mieux assurer que les services essentiels offerts ne soient pas interrompus dans le cas où ses bureaux deviendraient inutilisables.

Étude du CSARS : Activités de bureaux de district du SCRS dans des aéroports internationaux canadiens

CONTEXTE

Un réseau d'aviation civile sécuritaire et sûr constitue un rouage vital de l'économie canadienne. Sa sécurité revêt donc une grande importance. À la suite de l'attentat à la bombe commis en 1985 contre le vol 182 d'Air India et des attaques terroristes du 11 septembre, diverses mesures ont été prises à l'échelle canadienne pour améliorer la sûreté de l'aviation, dont de nouvelles règles pour la construction des avions et des aéroports, un filtrage amélioré des personnes et des biens dans les aéroports, l'obligation faite aux transporteurs aériens de communiquer des renseignements de base sur des passagers ou des vols particuliers et l'affectation de policiers banalisés à bord des avions canadiens pour en assurer la sécurité. La liste de ces initiatives n'est pas exhaustive, mais elle illustre l'évolution de la sûreté de l'aviation civile en un vaste réseau d'intervenants et de responsabilités auquel participent les organismes régionaux, provinciaux et fédéraux ainsi que les transporteurs aériens et les agences privées de sécurité.

L'ÉTUDE DU CSARS

Par ses enquêtes sur les menaces à la sécurité nationale et ses évaluations de sécurité des voyageurs qui viennent au Canada ou des employés d'aéroport devant avoir accès à des zones réglementées, le SCRS joue un rôle essentiel au sein du réseau complexe d'intervenants dans la sécurité des aéroports. Les activités du SCRS dans les aéroports canadiens soutiennent le cadre de sûreté de l'aviation dans leurs régions respectives. Pour cette étude, le CSARS a examiné les activités du SCRS dans certains aéroports canadiens. L'idée était de mieux comprendre et évaluer le rôle que le SCRS y joue, y compris la manière dont il gère ses responsabilités ayant trait aux aéroports et dont il travaille avec ses partenaires sur place. Par un contact constant avec les intervenants des aéroports, le personnel du Service peut transmettre de l'information aux régions et à l'Administration centrale et il sert d'intermédiaire dans la collecte et le partage d'informations entre les partenaires dans les aéroports. L'efficacité de leurs communications dépend de la solidité de leurs relations. Le CSARS a remarqué que les deux bureaux de district avaient consacré pas mal de temps et d'efforts à tisser et à cultiver les rapports avec les intervenants des aéroports, à la fois ceux du gouvernement et de l'extérieur de celui-ci.

De plus, le CSARS a remarqué que le gouvernement et les partenaires du maintien de l'ordre en milieu aéroportuaire demandent souvent conseil au personnel du SCRS affecté aux aéroports, pour ce qui touche la sécurité nationale, relativement aux activités qui s'y

Cette position place le SCRS en position d'incertitude et de vulnérabilité en cas de poursuites judiciaires, comme on l'a vu dans l'affaire Omar Khadr. En effet, les tribunaux canadiens avaient alors conclu que le MAFCI et le SCRS avaient violé les droits de M. Khadr, selon la *Charte*, en s'entretenant avec lui et en présentant aux enquêteurs américains les informations obtenues. Le message des tribunaux est donc que le SCRS ne peut plus mener ses activités dans l'optique limitée de la collecte de renseignements. Il doit aussi examiner le contexte plus vaste et les implications de l'exercice de son travail.

Experts du renseignement et universitaires s'entendent pour dire que le monde du renseignement a changé radicalement depuis le 11 septembre. Le SCRS a pris des mesures importantes pour relever certains défis suscités par la suite, mais l'affaire Omar Khadr donne à penser que les changements aux politiques et aux procédures ne sont qu'un élément de la transition plus profonde qui doit s'opérer.

Le temps est peut-être venu, pour le SCRS, de réévaluer en profondeur la manière dont il mène ses activités et d'amorcer un changement culturel afin de se tenir au diapason des progrès politiques et juridiques des dernières années. Il importe aussi qu'il démontre qu'il a le professionnalisme, l'expérience et le savoir-faire nécessaires à la prise des décisions difficiles qui s'imposent dans la conduite d'opérations à l'étranger. En effet, le SCRS est l'objet de pressions et d'attentes de plus en plus grandes l'incitant à examiner les questions étrangères au renseignement dans l'exercice de son mandat et de ses activités.

SOMMAIRE DES RECOMMANDATIONS

Cette étude contient deux recommandations :

- Le Service devrait songer à élaborer un cadre stratégique destiné à guider ses interactions auprès des jeunes. Dans ce cadre-là, il devrait veiller à ce que ces interactions se fondent sur le même type de principes que ceux consacrés en droit canadien et international.
- Le SCRS devrait instaurer des mesures pour intégrer dans son travail courant les valeurs découlant des faits récents sur la scène politique, judiciaire et juridique, afin de maintenir sa propre crédibilité et de combler les attentes croissantes et changeantes quant aux modalités d'opération et de rendement d'un service de renseignement dans une société démocratique contemporaine. Les conseils et l'assistance du ministre de la Sécurité publique seraient utiles quant à la manière de s'acquitter de cette tâche.

des efforts à l'échelle gouvernementale pour régler les questions relevant des affaires consulaires et relatives à la détention de Canadiens à l'étranger, dans des affaires de terrorisme ou des cas liés à la sécurité nationale. Le CSARS espère que ces faits nouveaux aideront dorénavant le SCRS à remplir sa tâche de collecte de renseignements tout en respectant les droits de la personne, en particulier dans les situations semblables à celle de M. Khadr.

Le deuxième point concerne l'âge de M. Khadr. En droit canadien et international, il est notoire que les jeunes jouissent de certains droits fondamentaux en raison de leur statut de mineurs. Au Canada, ce principe est inscrit dans la *Loi sur le système de justice pénale pour les adolescents*, adoptée par le gouvernement fédéral. Les droits des enfants sont aussi affirmés dans des conventions internationales auxquelles le Canada est partie, telle la *Convention des Nations Unies relative aux droits de l'enfant*.

Le CSARS n'a trouvé aucune preuve que le SCRS ait tenu compte du fait que M. Khadr était encore jeune lorsqu'il a décidé de le voir en entrevue à Guantanamo Bay. De plus, la radicalisation des jeunes préoccupe de plus en plus le Service. À la lumière de ces faits, le CSARS a recommandé au SCRS de songer à établir un cadre stratégique destiné à guider ses interactions auprès des jeunes. Dans ce cadre-là, il devrait veiller à ce que ces interactions se fondent sur le même type de principes que ceux consacrés en droit canadien et international.

En général, le CSARS croit que le partage d'informations avec les pays qui ont de mauvais antécédents en matière de respect des droits de la personne restera difficile pour le SCRS tant que le gouvernement du Canada n'aura pas réglé sa position apparemment contradictoire, touchant les renseignements arrachés sous la torture, par rapport aux orientations qu'il donne au SCRS pour l'exécution de son travail.

PAS DE SOLUTIONS FACILES

Les questions soulevées dans cette affaire — tels l'échange d'informations avec des partenaires étrangers et les questions liées aux droits de la personne quand on traite avec des jeunes et qu'on interagit avec des détenus dans des pays étrangers — ne comportent ni réponses ni solutions faciles. De nouveaux mécanismes ont été établis pour inciter le SCRS à tenir compte de ces questions dans le cadre de son processus décisionnel. Cependant, de l'avis du CSARS, il devient manifeste que la recherche de solutions à nombre de ces questions complexes, ultérieures au 11 septembre, obligera à repenser à fond le travail du renseignement à la lumière des récentes réalités sociopolitiques et juridiques.

En conséquence, le CSARS estime que le SCRS n'a pas porté l'attention requise à deux points importants, étrangers au renseignement : les questions entourant les droits de la personne et l'âge de M. Khadr au moment de son entrevue avec le SCRS.

Le gouvernement du Canada appuyait en tous points la visite et l'entrevue du SCRS avec M. Khadr à Guantanamo Bay en février 2003, car cette initiative s'inscrivait dans une approche pangouvernementale visant à permettre un entretien avec lui pendant sa détention.

de la personne. Les échanges et la coopération du SCRS avec les partenaires étrangers sont scrutés de plus près depuis le 11 septembre, car il est devenu manifeste que les services de renseignement doivent travailler de concert pour faire échec aux menaces terroristes qui transcendent les frontières géopolitiques. La communication d'informations aux partenaires étrangers est essentielle à l'exécution du mandat du SCRS, mais elle a suscité de nouvelles difficultés, en particulier lorsqu'il traite avec des pays qui ne partagent pas le respect du Canada pour les droits de la personne.

À l'époque des entrevues du SCRS avec M. Khadr, en février 2003, une foule de reportages médiatiques ont fait état d'allégations de mauvais traitements et d'abus dont étaient victimes les détenus sous garde américaine, en Afghanistan et à Guantanamo Bay. Au milieu de 2002, plusieurs individus ont fait des allégations quant au traitement que les soldats américains leur avaient réservé, après avoir été emmenés sous garde en Afghanistan à la fin de 2001 et en 2002. Entre-temps, l'établissement américain de détention de Guantanamo Bay a ouvert ses portes dans la controverse, car bien des pays ont dénoncé le traitement judiciaire réservé aux détenus par les États-Unis et la façon dont ce pays les avait traités.

Le CSARS n'a trouvé aucune preuve que le SCRS ait tenu compte de ces informations lorsqu'il a décidé de s'entretenir avec M. Khadr.

Par suite de recommandations formulées par le CSARS en 2004 et par le juge O'Connor en 2006 au sujet de l'affaire Maher Arar, le SCRS a examiné ses politiques régissant les circonstances où il échange des informations avec des partenaires étrangers dont les antécédents semblent douteux en matière de respect des droits de la personne. Le SCRS et le ministère des Affaires étrangères et du Commerce international (MAECI) ont aussi signé en 2007 un nouveau protocole visant à assurer une coordination et une cohérence accrues

POUVOIR LÉGAL DU CSARS
DANS CETTE AFFAIRE

L'étude du CSARS sur le rôle joué par le SCRS dans l'affaire Omar Khadr a été menée en vertu de l'article 54 de la Loi sur le SCRS, qui autorise le Comité à présenter au ministre de la Sécurité publique un rapport spécial sur toute question ayant trait à l'exercice des fonctions du SCRS par celui-ci. La plupart du temps, ces rapports se limitent aux questions qui posent des problèmes particulièrement épineux ou très médiatisés et que le CSARS estime devoir être portées directement à l'attention du Ministre. Voici quelques exemples de précédentes études du CSARS en vertu de l'article 54 : l'affaire Mohammed Mansour Jabarah, celle concernant Maher Arar, l'affaire du Héritage Front et les activités du SCRS relativement à l'attentat à la bombe commis contre le vol 182 d'Air India.

Le motif déterminant de l'intérêt du SCRS à avoir une entrevue avec M. Khadr était de recueillir des renseignements de sécurité sur une menace peut-être grave et de conseiller le gouvernement du Canada en conséquence. Le CSARS comprend la position du SCRS — soit qu'il avait des motifs raisonnables de se rendre à Guantanamo Bay pour recueillir des informations liées à la menace — mais il a constaté que la décision du Service de s'entretenir avec M. Khadr reposait surtout sur des motifs liés au renseignement. Le Service a profité de l'occasion pour recueillir des renseignements de nature à faire avancer sa propre enquête.

L'objectif du CSARS était d'effectuer une étude approfondie sur la participation du SCRS dans l'affaire Omar Khadr. Le Comité est remonté jusqu'au milieu d'août 2002 — moment où les autorités américaines ont informé les responsables canadiens, dont le SCRS, que les forces américaines avaient capturé M. Khadr — jusqu'à l'époque de l'injonction de la Cour fédérale, en septembre 2005, qui a interdit aux autorités canadiennes de revoir M. Khadr en entrevue.

ÉTUDE DU CSARS

SCRS à Guantanamo Bay, en février 2003. Cette bande a suscité des questions sur la scène publique quant à la nature et à la portée de la participation du SCRS dans cette affaire, y compris les motifs qui l'ont guidé dans sa décision de rencontrer M. Khadr.

LA REDDITION DE COMPTES IMPORTE

Le CSARS est l'un des divers mécanismes conçus pour assurer la reddition de comptes au sujet du SCRS. Outre les études et les enquêtes sur les plaintes effectuées par le Comité, le Service doit aussi faire rapport de ses opérations par l'entremise du ministre de la Sécurité publique, des tribunaux, de l'inspecteur général du SCRS, des organismes centraux du gouvernement (p. ex. le Bureau du Conseil privé et le Secrétaire du Conseil du Trésor), du vérificateur général ainsi que des commissaires à l'information et à la protection de la vie privée du Canada.

Chaque étude est un instantané des actions du Service dans un contexte particulier. Cette approche permet au Comité de gérer le risque que comporte le fait de ne pouvoir examiner qu'un petit nombre des activités du SCRS une année donnée.

Les chercheurs du CSARS consultent diverses sources d'information, qui varient selon les études, lorsqu'ils se penchent sur des aspects particuliers des travaux du Service. Dans ce processus, ils peuvent organiser des séances d'information avec des employés du SCRS et étudier les dossiers d'enquête sur des individus et des groupes, les dossiers de sources humaines, les évaluations de renseignements et les documents joints aux mandats ainsi que les dossiers ayant trait à la coopération et aux échanges opérationnels du SCRS avec des organismes et des partenaires canadiens et étrangers. L'idée de cette multiplicité de sources est de créer un tel corpus varié d'informations que le CSARS soit assuré d'examiner et de comprendre à fond les dossiers en cause.

Étude du CSARS : Rôle joué par le SCRS dans l'affaire Omar Khadr

CONTEXTE

Nombre de Canadiens connaissent bien l'histoire d'Omar Ahmed Khadr, ce citoyen canadien qui a été détenu dans l'établissement américain de Guantanamo Bay et accusé d'avoir tué un médecin de l'armée des États-Unis lors d'un échange de coups de feu en Afghanistan, en 2002. Divers sujets, dont la cause judiciaire des États-Unis contre M. Khadr, le traitement qu'ils lui ont réservé pendant qu'il était sous leur garde, son statut à titre d'enfant-soldat et la position du gouvernement canadien concernant son rapatriement, ont suscité de nombreux reportages médiatiques et des commentaires. En juillet 2008, l'histoire de M. Khadr a occupé la scène internationale lorsque ses avocats ont rendu publique une bande vidéo montrant leur client en entrevue avec des représentants du

SECTION 2 : RÉSUMÉS DES ÉTUDES DU CSARS ET DES PLAINTES

A. ÉTUDES

Depuis plus de 25 ans, les études du CSARS fournissent au Parlement et aux Canadiens un tableau complet des activités opérationnelles du Service. Elles visent aussi à déterminer si le Service exerce ses fonctions dans les règles, avec efficacité et dans le respect de la loi. Les études du CSARS fournissent un examen rétrospectif et une évaluation d'enquêtes et de fonctions particulières du SCRS. Elles contiennent des constatations et, s'il y a lieu, des recommandations visant le Service. Une fois terminées, toutes les études sont remises à la fois au directeur et à l'inspecteur général du SCRS. Le CSARS est aussi autorisé à présenter des rapports spéciaux au ministre de la Sécurité publique sur toute question qu'il estime d'importance spéciale ou que le Ministre lui demande d'étudier.

Le programme de recherches du CSARS est conçu de manière à englober un vaste éventail de sujets. Lorsqu'il détermine ceux qu'il examinera, le CSARS prend en considération :

- les événements susceptibles de menacer la sécurité du Canada;
- les activités particulières du SCRS qui pourraient porter atteinte aux droits et libertés individuels;
- les priorités et préoccupations qui sont énoncées par le Parlement ou dans les médias;
- les questions cernées par le Comité dans l'exercice de ses fonctions relatives aux plaintes; les nouvelles orientations ou initiatives annoncées par le SCRS ou le touchant;
- le rapport annuel classifié que le directeur du SCRS présente au ministre de la Sécurité publique;
- la nécessité d'évaluer régulièrement chacune des directions du Service et chacun de ses bureaux régionaux.

ÉTUDES ANTÉRIEURES DU CSARS

Au fil des ans, le CSARS a examiné un vaste éventail des activités du SCRS. Ainsi, il s'est penché sur la manière dont le Service remplit son mandat à l'étranger en scrutant les activités menées dans ses divers postes autour du monde, les activités et les enquêtes des bureaux régionaux du SCRS, la coopération et les échanges de renseignements de celui-ci avec ses partenaires canadiens et étrangers et des activités opérationnelles particulières, tel le recours aux sources humaines par le SCRS. La liste complète des études antérieures du CSARS peut être consultée sur son site Web (www.sirc-csars.gc.ca).

Le CSARS a le pouvoir de se prononcer sur la manière dont le SCRS exerce ses pouvoirs et de déterminer si ceux-ci sont justes, raisonnables et proportionnels à la menace. Dans son étude sur les Services techniques et scientifiques du SCRS, le Comité a mentionné le silence continu de la législation au sujet de l'accès légal, et les effets de ce silence sur les opérations du Service. Une telle loi s'impose. Elle obligerait les fournisseurs de services Internet à doter leurs réseaux d'une capacité d'interception. Le CSARS espère que les tout derniers efforts d'ordre législatif, déployés par le gouvernement à l'égard de cette question, permettront d'atteindre cet objectif.

Le rôle du CSARS à titre d'organisme de surveillance serait simple s'il était possible d'analyser des succès et des échecs du domaine public afin d'en tirer des leçons. Comme nous avons la chance qu'il n'y ait pas eu d'attentat réel ou d'incident majeur sur le plan de la sécurité, le CSARS examine les aspects des opérations du SCRS qui pourraient servir d'indicateurs valables de la capacité de celui-ci, de son efficacité et de son efficacité. Dans le passé, le CSARS a concentré une bonne partie de ses activités de surveillance sur les opérations du SCRS au Canada. Au moment où le SCRS s'apprête à étendre sa capacité d'œuvrer hors du pays, il faudra donc que le CSARS affecte davantage de ressources à surveiller ces activités. De plus, il continuera d'enquêter sur les plaintes, pour déterminer non seulement si elles sont justifiées, mais si elles indiquent des problèmes plus systémiques à scruter.

En raison de ses vastes pouvoirs d'investigation au sujet du SCRS, le CSARS prend très au sérieux la tâche de comprendre les défis complexes que le SCRS doit relever et d'examiner à fond les activités de celui-ci.

Le rapport annuel du CSARS est l'une des tâches essentielles qui concourent à combler cette attente, tâche que le Parlement lui a confiée au nom des Canadiennes et des Canadiens.

Selon le CSARS, il est important que le SCRS se penche sur les nombreux problèmes qui se posent dans le travail du renseignement de sécurité au sein d'une société démocratique contemporaine. Par-dessus tout, bien que la collecte de renseignements de sécurité soit la raison d'être du Service, l'affaire Khadr souligne à quel point les questions étrangères au renseignement doivent devenir partie intégrante des processus décisionnels du SCRS. Dans le cadre de cette transition, celui-ci doit miser sur les directives du Ministre, en plus de ses propres expérience et ressources.

Dans une étude distincte, le Comité a examiné les activités du SCRS dans les aéroports canadiens. Ceux-ci peuvent être la cible d'attaques terroristes du fait qu'on y trouve de fortes concentrations de gens et qu'ils sont un chaînon vital de l'infrastructure canadienne de transport. Par ces activités, le SCRS soutient le cadre de sûreté de l'aviation en prodiguant des conseils à l'égard de la sécurité nationale et en voyant en entrevue des personnes soupçonnées de représenter une menace pour la sécurité. L'étude des activités du Service à ces aéroports a permis au CSARS de constater que la présence du SCRS améliore le contexte de la sécurité.

Le CSARS a aussi examiné les effets que la loi fédérale adoptée après le 11 septembre, intitulée *Loi antiterroriste* (2001), a eus sur les activités du SCRS. À titre d'exemple, l'un des objectifs de cette loi est la lutte au financement du terrorisme. Cependant, cette loi a suscité de grandes difficultés au SCRS dans la gestion de son programme des sources humaines. En particulier, en raison des dispositions qu'elle renferme, les activités reliées à ce programme et susceptibles de bénéficier à des organisations inscrites à titre d'entités terroristes peuvent être des actes criminels, par définition. Le SCRS a pris des mesures à cet égard, mais le CSARS estime qu'une reddition de comptes plus poussée au ministre de la Sécurité publique s'impose au sujet de certains aspects du programme des sources humaines du Service.

Dans son étude concernant l'enquête du SCRS sur l'extrémisme intérieur, le CSARS a constaté qu'il y avait lieu de revoir et de reformuler des éléments clés de la stratégie du Service à l'égard du contexte de la menace intérieure. Il estime nécessaire de veiller à ce qu'il y ait une compréhension claire et commune à la fois du contexte de la menace et des termes employés pour le décrire. Cette tâche deviendra plus pressante au cours des prochains mois, à l'approche des Jeux olympiques et paralympiques d'hiver qui se tiendront en 2010 à Vancouver et qui seront une épreuve de taille pour l'infrastructure de sécurité du Canada.

Lorsque les services de sécurité sont aux prises avec un contexte de la menace multidimensionnel et qu'il faut maintenir la nécessité de protéger les valeurs fondamentales de la société, le rôle d'un organisme de surveillance est tout aussi complexe. Le CSARS doit se prononcer sur la capacité du SCRS à exécuter son mandat et sur les outils dont il dispose pour exécuter son travail. Fait tout aussi important, les recommandations du CSARS doivent être concrètes et refléter les valeurs des Canadiens.

Le CSARS est le seul organisme indépendant, de l'extérieur, à être investi du mandat de se prononcer sur les divers aspects des opérations du Service. Il peut donner suite aux plaintes ou, de sa propre initiative, se pencher sur des aspects particuliers du SCRS. Il peut aussi répondre aux demandes du ministre de la Sécurité publique l'invitant à examiner l'exercice des fonctions du SCRS par celui-ci.

Chaque année, le CSARS scrute une gamme d'activités opérationnelles du Service afin de déterminer s'il les a exécutées dans les règles, avec efficacité et dans le respect de la loi. Le rapport annuel de cette année couvre un éventail de ces activités et traite de certaines questions complexes auxquelles se heurte le Service. La section 2 du présent rapport résume les études du Comité et sa décision à l'égard d'une plainte.

De l'avis du CSARS, le SCRS a fait des progrès importants dans l'élaboration de politiques destinées à lui servir de guide au sujet des questions liées aux droits de la personne qui se posent dans ses enquêtes sur les menaces à la sécurité nationale. Comme le révèle cependant l'étude du CSARS sur le rôle joué par le SCRS dans l'affaire Omar Khadr, il y a aussi d'autres questions à examiner. En particulier, le SCRS doit prendre en considération les principes du droit national et international relatifs au traitement réservé aux mineurs lorsqu'il voit en entrevue un Canadien détenu à l'étranger.

Les services de sécurité ne peuvent enquêter sur les activités terroristes, à moins d'échanger efficacement des informations avec l'étranger. Certains pays pouvant disposer de renseignements vitaux sur les menaces à la sécurité du Canada ne respectent pas les droits de la personne qui tiennent à cœur aux Canadiens. Le Canada ne recourt pas à la torture ni n'approuve ceux qui le font. Il est cependant moins simple de dire si le SCRS devrait coopérer et traiter avec des pays qui violent peut-être les droits de la personne pour obtenir des renseignements liés à la menace. Il importe donc de plus en plus que le CSARS examine les interactions du Service avec les services de renseignement étrangers. Une question connexe se pose si un représentant du SCRS voit en entrevue un Canadien détenu à l'étranger. Pour le SCRS, la priorité est de recueillir des renseignements de sécurité. Parallèlement, il doit prendre en considération tout soupçon de recours à la torture et toute autre violation des droits de la personne, qu'un détenu puisse les confirmer directement ou non.

SECTION 1 : BILAN DE L'EXERCICE

En moins de deux décennies, le contexte mondial dans lequel baigne le renseignement de sécurité canadien a subi une transformation radicale.

La fin de la guerre froide a fait miroiter la promesse d'un monde plus pacifique, fort d'un nombre croissant de démocraties et d'une prospérité économique plus répandue. On a tôt fait de comprendre, cependant, que le nouveau contexte mondial était à la fois plus complexe et moins sûr qu'à l'époque où les intérêts de l'Occident se démarquaient clairement de ceux du monde communiste.

La montée du terrorisme mondial, marquée principalement par l'ascension d'Al-Qaïda à titre de plateforme terroriste d'envergure mondiale, a joué un rôle important pour ce qui est de façonner le monde d'aujourd'hui. Les attaques du 11 septembre contre les États-Unis et les attentats perpétrés par la suite en Europe et en Asie ont modifié la manière dont les pays du monde entier perçoivent le potentiel destructeur du terrorisme et y font face.

Le contexte contemporain de la menace se caractérise par un risque constant d'attaques méticuleusement préparées pour effrayer et pour causer des pertes massives et détruire les infrastructures. Al-Qaïda a menacé ouvertement de s'en prendre au Canada. Notre pays a aussi été touché par des cellules terroristes intérieures qui se radicalisaient. L'arrestation et le procès de membres de la cellule « Toronto 18 » reflètent le contexte de cette menace complexe et changeante.

Le CSARS reconnaît que le SCRS doit faire face à ces menaces terroristes tout en poursuivant ses priorités traditionnelles en matière de contre-espionnage. Par exemple, les enquêtes sur les implications clandestines de gouvernements étrangers sur le plan de la sécurité nationale demeurent une importante préoccupation. De même, la lutte contre la prolifération reste l'une des toutes premières priorités du SCRS au moment où la communauté internationale est aux prises avec divers régimes instables qui nourrissent des ambitions nucléaires.

Tout comme le contexte de la menace dans lequel le SCRS évolue, le contexte juridique correspondant subit également des changements. Des poursuites judiciaires récentes ont levé le voile sur les rouages internes de la collectivité du renseignement. Dans le cadre de ce processus, des décisions judiciaires ont obligé à veiller à ce que les renseignements fournis aux tribunaux par le SCRS respectent les plus hautes normes juridiques.

Le CSARS croit que le contexte du renseignement de sécurité demeurera caractérisé par la multiplicité des menaces et par une profonde imprévisibilité. Il se peut que la polarisation du terrorisme mondial évolue, mais on peut s'attendre à ce qu'il continue de semer le désordre et l'instabilité. Dans ce contexte, pour prévoir et désamorcer les projets terroristes tout en enquêtant sur les autres menaces à la sécurité nationale, il faut un service de renseignement de sécurité efficace.

NOUVELLE ALLURE DU RAPPORT ANNUEL DU CSARS

Dans la foulée des efforts constants du CSARS pour comprendre les nouveaux défis et responsabilités en matière de renseignement de sécurité au Canada, et pour faire rapport à ce sujet, une nouvelle présentation a été donnée à son rapport annuel. Voici les éléments clés de ces changements :

UNE ANALYSE PLUS APPROFONDIE DU CSARS
Dans ce rapport de présentation différente, le CSARS explore le contexte en évolution dans lequel baigne le renseignement de sécurité. On y trouve des observations au sujet des tendances et défis clés auxquels le SCRS devra faire face au cours des prochaines années.

UNE RÉFÉRENCE FACILE AUX FAITS ET AUX RECOMMANDATIONS
La nouvelle présentation du rapport vise à aider le lecteur à trouver les faits et renseignements qu'il cherche, y compris les recommandations formulées pendant la période à l'étude et des renseignements importants sur le Comité.

DES RENSEIGNEMENTS DE BASE LÀ OÙ IL FAUT
Reportez-vous aux encadrés tout au long du rapport. Ils contiennent des renseignements de base utiles sur diverses questions d'ordre juridique et stratégique qui concernent les fonctions du CSARS en matière de surveillance et d'étude des plaintes.

A PROPOS DU PRÉSENT RAPPORT

Le CSARS fournit l'assurance au Parlement, et par son entremise aux Canadiens, que le SCRS enquête sur les menaces à la sécurité nationale d'une façon qui respecte la primauté du droit et les droits des Canadiennes et des Canadiens, et qu'il fait rapport à ce sujet.

La Loi sur le SCRS confère au CSARS un droit d'accès à toutes les informations qui relèvent du Service. En conséquence, le CSARS peut se pencher sur tous les dossiers et sur toutes les activités du Service, quel que soit le niveau de classification de l'information en cause. Les documents confidentiels du Cabinet (c.-à-d. les communications écrites et verbales qui contribuent à la prise des décisions collectives des ministres) sont l'unique exception à cette règle.

Le présent rapport annuel résume les principales analyses du CSARS ainsi que les constatations et recommandations qui découlent de ses études et de ses enquêtes sur les plaintes. Il compte trois sections :

SECTION 1 : BILAN DE L'EXERCICE

Une analyse des nouveaux faits marquants dans le milieu du renseignement de sécurité, et de leurs rapports avec les constatations et recommandations formulées par le CSARS lors du dernier exercice.

SECTION 2 : RÉSUMÉS DES ÉTUDES DU CSARS ET DES PLAINTES

Un résumé des études effectuées par le CSARS et des rapports de plainte qu'il a présentés durant la période visée dans le présent rapport.

SECTION 3 : SURVOL DU CSARS

Description détaillée des activités de rayonnement et de liaison du CSARS, et de ses activités d'ordre administratif, y compris son budget annuel et ses dépenses.

Arthur T. Porter, C.P., M.D. Il nous tarde à tous de servir les Canadiens et les Canadiennes avec l'engagement même que caractérisent les travaux du CSARS depuis sa création. Les membres du Comité aimeraient aussi manifester leur gratitude à leurs collègues dont le mandat a pris fin récemment : l'honorable Roy Romanow, C.P., O.C., c.r., l'honorable Baljit S. Chadha, C.P., et l'honorable Alda Landry, C.P., C.M., c.r. Nous les remercions de leur dévouement et leur souhaitons tout le succès possible dans leurs projets futurs.

Enfin, les membres du Comité aimeraient profiter de l'occasion pour présenter leurs meilleurs vœux à M. Jim Judd qui a quitté la fonction publique en juin 2009 après avoir exercé les fonctions de directeur du SCRS. Selon nous, M. Judd a guidé consciencieusement le Service dans certains des dossiers les plus complexes qu'il a été donné à celui-ci de traiter ces dernières années. Tous les membres du CSARS le remercient de son professionnalisme lors des diverses occasions qu'il a eues de discuter avec eux des travaux du SCRS et de l'état du renseignement de sécurité. Nous anticipons le plaisir de travailler avec son successeur, M. Richard B. Fadden, et lui souhaitons bonne chance dans son nouveau poste.

Nous sommes fiers de présenter, au Parlement et à tous les Canadiens, les résumés des études et des enquêtes sur les plaintes que nous avons effectuées en 2008-2009. Nous espérons que le présent rapport annuel contribuera à les éclairer sur le rôle et les responsabilités du CSARS et sur son apport constructif afin d'assurer que le SCRS est efficace dans ses enquêtes et ses rapports sur les menaces à la sécurité nationale, travaux qu'il effectue dans le respect des droits et des libertés des citoyens. C'est là une partie intégrante du plan de responsabilisation que le Parlement a établi en 1984 — un cadre qui a résisté à l'épreuve du temps et une responsabilité qu'il nous tarde de continuer d'exercer avec beaucoup de fierté.



Le président du Comité, Arthur T. Porter, C.P., M.D., avec les membres du Comité : Roy Romanow, C.P., O.C., c.r., Alda Landry, C.P., C.M., c.r., et Baljit S. Chadha, C.P.

MESSAGE DES MEMBRES DU COMITÉ

Le renseignement de sécurité baigne dans un contexte en évolution constante. Depuis plusieurs décennies, la nature et le rythme de cette évolution ont pris une ampleur sans précédent au Canada et ailleurs. Face au contexte diversifié de la menace de la part d'États aussi bien que de protagonistes non étatiques et devant les enquêtes de plus en plus nombreuses à l'étranger, la demande grandissante d'intervenants étatiques et les nombreuses enquêtes publiques et décisions judiciaires qui ont trait à la sécurité nationale, le monde du renseignement de sécurité est devenu de plus en plus complexe.

C'est sur cette toile de fond que le Comité de surveillance des activités de renseignement de sécurité (CSARS ou Comité) continue de servir les Canadiens afin d'assurer la reddition de comptes démocratique de l'un des organismes gouvernementaux les plus impénétrables du pays. Le mandat du CSARS demeure étroitement lié à la prestation, au Parlement, de l'assurance que le Service canadien du renseignement de sécurité (SCRS ou Service) enquête sur les menaces à la sécurité nationale, d'une façon qui respecte la primauté du droit et les droits des Canadiennes et des Canadiens, et qu'il fait rapport à ce sujet. Cependant, l'éventail des questions liées au renseignement de sécurité qu'il nous faut comprendre et examiner continue d'évoluer quant à leur nature et à leur portée.

Nous, membres du CSARS, sommes très fiers de faire partie d'un organisme qui déploie tout l'éventail des outils dont il dispose pour remplir son mandat. Par la *Loi sur le Service canadien du renseignement de sécurité (Loi sur le SCRS)*, le Parlement a confié au Comité le vaste mandat d'examiner l'exercice des fonctions du SCRS par celui-ci. Depuis sa création dans les années 80, le CSARS s'est employé à exercer cette responsabilité en suivant l'évolution des priorités du SCRS et des attentes nouvelles des Canadiens à l'égard du renseignement de sécurité dans une société démocratique. Selon le Comité, la *Loi sur le SCRS* lui a fourni un cadre modèle pour l'exécution de son mandat.

Notre rapport annuel est un rouage vital de nos efforts pour satisfaire à ces attentes en maintenant la fière tradition qui consiste à renseigner et à analyser avec probité et équité. Étant donné la nature et la portée des changements au contexte du renseignement de sécurité, nous croyons que cette entreprise est un moment approprié pour offrir aux Canadiens une nouvelle approche au rapport de nos constatations et de nos recommandations.

Le rapport annuel de cette année compte une section « analyse » qui énonce les grands thèmes examinés par le CSARS au cours du dernier exercice et qui incite le lecteur à soupeser l'importance de la reddition de comptes en cette ère nouvelle du renseignement de sécurité. Nous sommes confiants que cette entreprise donnera au Parlement et à tous les Canadiens un regard neuf sur le rôle du CSARS dans la surveillance des opérations du SCRS.

Le CSARS lui-même a aussi connu d'importants changements au cours de la dernière année. Nous avons accueilli récemment trois nouveaux membres au sein du Comité : l'honorable Frances Lankin, C.P., l'honorable Denis Losier, C.P., et l'honorable

TABLE DES MATIÈRES

2	MESSAGE DES MEMBRES DU COMITÉ
4	À PROPOS DU PRÉSENT RAPPORT
6	SECTION 1 : BILAN DE L'EXERCICE
10	SECTION 2 : RÉSUMÉS DES ÉTUDES DU SCRS
10	ET DES PLAINTES
10	A. ÉTUDES
11	Rôle joué par le SCRS dans l'affaire Omar Khadr
16	Activités de bureaux de district du SCRS dans des aéroports internationaux canadiens
18	Opération du SCRS faisant appel à des sources humaines
19	Activités du SCRS dans un poste à l'étranger
21	Services techniques et scientifiques du SCRS
23	Enquête du SCRS sur l'extrémisme intérieur
24	L'affaire Paul William Hampel
26	B. PLAINTES
28	Enquête sur une affaire de profilage présumé
30	SECTION 3 : SURVOL DU CSARS
30	Activités du Comité
30	Composition du Comité
30	Personnel et organisation
31	Budget et dépenses
32	ANNEXE A : LISTE DES RECOMMANDATIONS
33	ANNEXE B : SURVOL DU SCRS
33	A. ACTIVITÉS EN MATIÈRE DE RENSEIGNEMENT
33	DE SÉCURITÉ
33	Ciblage
34	Mandats
34	B. ACTIVITÉS EN MATIÈRE D'ÉVALUATION DE SÉCURITÉ
34	Evaluations de sécurité pour le gouvernement
36	Evaluations de sécurité en vue de l'accès à des sites
37	Evaluations de sécurité à l'immigration

QU'EST-CE QUE LE SCRS?

Le SCRS a charge de recueillir des renseignements de sécurité et d'autres informations connexes, tant au Canada qu'à l'étranger, et de les analyser. Il conseille le gouvernement du Canada au sujet des questions et activités qui menacent la sécurité nationale. Le SCRS effectue également des évaluations de sécurité pour le compte de tous les ministères et organismes fédéraux, sauf la Gendarmerie royale du Canada. Pour plus de renseignements sur certaines activités clés du SCRS, veuillez vous reporter à l'annexe B du présent rapport annuel.

QU'EST-CE QUE LE CSARS?

Le Comité de surveillance des activités de renseignement de sécurité (CSARS ou Comité) est un organisme indépendant qui rend compte au Parlement du Canada au sujet des opérations du Service canadien du renseignement de sécurité (SCRS ou Service). L'examen des activités du SCRS par le CSARS et les enquêtes qu'il effectue à l'égard des plaintes lui permettent de fournir au Parlement l'assurance que le Service enquête sur les menaces à la sécurité nationale d'une façon qui respecte la primauté du droit et les droits des Canadiennes et des Canadiens, et qu'il fait rapport à ce sujet.



Le 30 septembre 2009

L'honorable Peter Van Loan, C.P., député
Ministre de la Sécurité publique
Chambre des communes
Ottawa (Ontario)
K1A 0A6
Monseigneur le Ministre,

C'est pour nous un plaisir de vous remettre le rapport annuel du Comité de surveillance des activités de renseignement de sécurité pour l'exercice 2008-2009, tel qu'il est prescrit à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, afin qu'il soit transmis au Parlement.

Veuillez agréer, Monseigneur le Ministre, l'expression de notre haute considération.

Gary Filmon

Gary Filmon, C.P., O.M.

Président

Denis Losier

Denis Losier, C.P.

Raymond A. Speaker

Raymond Speaker, C.P., O.C.

Arthur T. Porter

Arthur T. Porter, C.P., M.D.

Frances Lankin

Frances Lankin, C.P.

Comité de surveillance des activités de renseignement de sécurité
B.P. 2430, succursale D
Ottawa (Ontario) K1P 5W5
613-990-8441

Veuillez consulter notre site électronique à www.sirc-csars.gc.ca

Les appels à frais vireés sont acceptés de 8 h à 17 h, heure normale de l'Est.

© Travaux publics et Services gouvernementaux Canada 2009

Numéro de catalogue PS 105-2009

ISBN 978-1-100-50024-9

La reddition de comptes en cette ère nouvelle du
renseignement de sécurité

Rapport annuel 2008-2009

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ



